2009-12

Rethinking the REAL ID Act and national identification cards as a counterterrorism tool

Clarke, William M.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

RETHINKING THE REAL ID ACT AND NATIONAL IDENTIFICATION CARDS AS A COUNTERTERRORISM TOOL

by

William M. Clarke

December 2009

Thesis Co-Advisors: Erik J. Dahl
Dorothy E. Denning

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2009	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Rethinking the REAL ID Act and National Identification Cards as a Counterterrorism Tool		**5. FUNDING NUMBERS**	
6. AUTHOR(S) William M. Clarke			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

The 9/11 Commission report described how driver's licenses, identification cards and travel documents are as important as weapons to terrorists. Vulnerabilities in existing identification systems provide the opportunity for illegal immigrants and terrorists to obtain driver's licenses and identification cards and once obtained these individuals can easily operate within the borders of United States. In response to the 9/11 Commission report, the federal government passed the REAL ID Act of 2005 (RIA), which established national standards for driver's licenses and identification card standards. But moving forward with implementing the RIA using the current defined standards may not be effective in addressing terrorism concerns. The RIA's guidelines require states to use a digital photograph on driver's licenses and identification cards as the primary biometric for identification. Photographs can be misleading because a person's physical appearance can change drastically due to hair loss, weight gain or change in hair color, making it difficult for law enforcement, Customs and Border Patrol officers and Transportation Security Administration personnel to positively identify individuals. Improvements in biometric technology allow for the incorporation of fingerprint, iris scan, hand geometry or detailed facial feature information in driver's license and identification card systems, and this thesis argues that incorporation of additional biometrics in driver's licenses and identification cards would improve national security. This thesis adds to the national identification card debate through an analysis of the RIA, an examination of the biometric identification technologies best suited for national security and border security purposes and an assessment of alternative biometric driver's license and identification cards.

14. SUBJECT TERMS REAL ID, PASS ID, Biometrics, Driver's License, Enhanced Driver's License, National Identification Card, Biometric Technologies, Fingerprints, Iris Scan, Facial Recognition, Hand Geometry, Department of Homeland Security	**15. NUMBER OF PAGES** 117
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

RETHINKING THE REAL ID ACT AND NATIONAL IDENTIFICATION CARDS AS A COUNTERTERRORISM TOOL

William M. Clarke
Major, United States Air Force
B.S., University of Rhode Island, 1994
M.S., University of Southern Mississippi, 1998

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2009**

Author: William M. Clarke

Approved by: Erik J. Dahl, PhD
Thesis Co-Advisor

Dorothy E. Denning, PhD
Thesis Co-Advisor

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The 9/11 Commission report described how driver's licenses, identification cards and travel documents are as important as weapons to terrorists. Vulnerabilities in existing identification systems provide the opportunity for illegal immigrants and terrorists to obtain driver's licenses and identification cards and once obtained these individuals can easily operate within the borders of United States. In response to the 9/11 Commission report, the federal government passed the REAL ID Act of 2005 (RIA), which established national standards for driver's licenses and identification card standards. But moving forward with implementing the RIA using the current defined standards may not be effective in addressing terrorism concerns. The RIA's guidelines require states to use a digital photograph on driver's licenses and identification cards as the primary biometric for identification. Photographs can be misleading because a person's physical appearance can change drastically due to hair loss, weight gain or change in hair color, making it difficult for law enforcement, Customs and Border Patrol officers and Transportation Security Administration personnel to positively identify individuals. Improvements in biometric technology allow for the incorporation of fingerprint, iris scan, hand geometry or detailed facial feature information in driver's license and identification card systems, and this thesis argues that incorporation of additional biometrics in driver's licenses and identification cards would improve national security. This thesis adds to the national identification card debate through an analysis of the RIA, an examination of the biometric identification technologies best suited for national security and border security purposes and an assessment of alternative biometric driver's license and identification cards.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAMVA	American Association of Motor Vehicle Administrators
ABIS	Automated Biometric Identification System
AETC	Air Education and Training Command
BFC	Biometrics Fusion Center
BMV	Bureau of Motor Vehicle
BTF	Biometrics Task Force
CAC	Common Access Card
CBP	Customs and Border Patrol
CER	Crossover Error Rate
DBIS	Defense Biometric Identification System
DEERS	Defense Enrollment Eligibility Reporting System
DHS	Department of Homeland Security
DoD	Department of Defense
DoS	Department of State
DMV	Department of Motor Vehicle
DTRA	Defense Threat Reduction Agency
EDL	Enhanced Driver's License
EER	Equal Error Rate
EPIC	Electronic Privacy Information Center
ESFS	Expeditionary Security Forces Squadron
FAR	False Acceptance Rate
FAST	Future Attribute Screening Technology

FBI	Federal Bureau of Investigation
FMR	False Match Rate
FRR	False Rejection Rate
FTC	Federal Trade Commission
FTE	Failure-to-Enroll
GAO	Government Accountability Office
HD	Hamming Distance
HSPD	Homeland Security Presidential Directive
IAFIS	Integrated Automated Fingerprint Identification System
ICAO	International Civil Aviation Organization
ICE	United States Immigration and Customs Enforcement
ID	Identification
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
IG	Inspector General
ISO	International Organization for Standardization
MEK	Mujahedin-e-Khalq
MRZ	Machine Readable Zone
NCSL	National Conference of State Legislatures
NGA	National Governors Association
NGIS	Next Generation Identification System
NIST	National Institute of Standards and Technology
NPRM	Notice of Proposed Rulemaking
NSPD	National Security Presidential Directive
NSPG	National Security Preparedness Group

PASS ID	Providing Additional Security in States Identification
PIN	Personal Identification Number
RFID	Radio Frequency Identification
RIA	Real ID Act of 2005
RSI	Recognition Systems, Inc.
SDSU	San Diego State University
SSN	Social Security Number
TCNS	Third-Country Nationals
TSA	Transportation Security Administration
U.S.	United States
USAF	U.S. Air Force
US-VISIT	United States Visitor and Immigrant Status Indicator Technology
WHTI	Western Hemisphere Travel Initiative

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my wife for her support during this lengthy process: without her support completion of this research would not have been possible. I am sincerely thankful to my thesis advisors, Professor Erik Dahl and Professor Dorothy Denning, for their encouragement, insight, expertise and challenging me to address hard questions.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PURPOSE AND IMPORTANCE OF THESIS

The purpose of this thesis is to review approaches to improving national security through better driver's licenses and identification cards. State-issued driver's licenses and identification cards are the most common form of identification used in the United States; typical uses include evidence that the holder has driving privileges, identity verification, age verification, address verification and automated administrative processing for government databases.[1] The lack of consistent driver's license and identification card standards among the states poses a problem when defending the U.S. from a possible terrorist attack. The success of federal, state and local agencies in protecting the U.S. from terrorist attack is in part dependent upon the ability of law enforcement agencies to effectively distinguish between citizens, legal residents, and those who may be in the U.S. illegally.

The 9/11 Commission Report recognized that driver's licenses, identification cards and travel documents are as important as weapons to terrorists.[2] Vulnerabilities in the existing identification systems provide the opportunity for illegal immigrants and terrorists to operate within the borders of the United States. Three of the five hijackers who crashed a plane into the Pentagon used fraudulently-obtained driver's licenses to board the plane and the pilot of the plane had four identification cards, all from different

[1] Department of Homeland Security, *REAL ID Act Regulatory Evaluation - Final Rulemaking,* Report Identification Number: 1601–AA37, Washington D.C.: DHS, January 17, 2008. 14.

[2] Jean Merserve and Mike Ahlers. *9/11 Commission Members Act to Finally Wrap it up,* July 25, 2009. http://www.cnn.com/2009/US/07/25/new.antiterror.group/index.html (accessed July 25, 2009).

states.[3] As stated by the 9/11 Commission, establishing and implementing national standards for driver's licenses and identification cards is a critical component to improving homeland security.[4]

This thesis investigates the current state of driver's licenses and identification cards through an examination of the Real ID Act of 2005 (RIA)[5] and an analysis of enhanced driver licenses. The RIA establishes minimum standards for driver's licenses and identification cards and requires states to verify an applicant's Social Security number, lawful immigration status and identity.[6] Enhanced driver's licenses were developed and implemented as a result of the Western Hemisphere Travel Initiative (WHTI).[7] Enhanced driver's licenses are an approved alternative travel document to a U.S. passport for reentry into the U.S. at land and sea borders with the U.S., Canada, Mexico and the Caribbean.[8]

After five years, the Department of Homeland Security (DHS) and states continue to struggle with implementation of the RIA. The DHS Secretary, Janet Napolitano, has indicated that it is time to assess whether to repeal the RIA.[9] State and federal officials have begun to reassess the RIA and evaluate new options for securing driver's licenses and identification cards. On July 15, 2009, the Senate Homeland Security and Government Affairs committee conducted a hearing to re-evaluate the RIA and debate

---

[3] 9/11 Commission, *9/11 and Terrorist Travel: Staff Report*, Franklin: Providence Publishing Company, August 2004, 39–44.

[4] 9/11 Commission, *The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States*, Washington D.C.: http://www.9-11commission.gov/report/911Report.pdf, 2004, 390.

[5] Division B—REAL ID Act of 2005, the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, Pub. L. 109-13, 119 Stat. 231, 302 (2005) (codified at 49 U.S.C. 30301).

[6] Department of Homeland Security, *REAL ID Act Regulatory Evaluation - Final Rulemaking*, Report Identification Number: 1601-AA37, Washington D.C.: DHS, January 17, 2008, 35.

[7] Section 7209 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458, 118 Stat. 3638, Dec 17, 2004) is referred to as the Western Hemisphere Travel Initiative (WHTI).

[8] Department of Homeland Security, *Enhanced Driver License: What are they?* June 2009. http://www.dhs.gov/xtrvlsec/crossingborders/gc_1197575704846.shtm (accessed July 23, 2009).

[9] CNN Washington D.C. Office. *Homeland Security Chief seeks to repeal REAL ID Act*, April 22, 2009, http://www.cnn.com/2009/POLITICS/04/22/real.ID.debate/ (accessed April 23, 2009).

the elements of new legislation sponsored by Democratic Senator Daniel Akaka from Hawaii entitled Providing Additional Security in States Identification (PASS ID).[10] Public debate is ongoing, and this thesis will add to the national discussion of the importance of securing driver's licenses and identification cards for national security.

B. PREVIEW OF ARGUMENT

The implementation of the RIA impacts everyone in the United States who holds a driver's license or identification card, requiring the re-issue of driver's license and identification cards to all 245 million current identification card holders.[11] But moving forward with implementation of the RIA, using the current DHS guidelines, may not be effective in addressing terrorism concerns. The RIA requires states to use digital photographs on driver's licenses and identification cards as the primary biometric for identification. This may be a problem, however, because an individual's physical appearance can change drastically because of weight loss, hair loss, weight gain, or a change in hair color, making it difficult for law enforcement or Transportation Security Administration (TSA) officers to positively identify individuals. Other biometric identification markers such as fingerprinting, iris scans, hand geometry and facial recognition may provide better capabilities for positive identification.

In addition, the Federal Bureau of Investigation (FBI) and law enforcement agencies have been using both photographs and fingerprints as an indicator of identity for decades. If the intent of standardizing driver's license and identification cards is to improve national security, then incorporating the latest biometric technology in identification systems may help to secure the homeland.

This thesis will examine how effective identification card technical solutions are in prohibiting terrorists and illegal immigrants from operating in the United States through a review of laws, technologies, issues and analysis of the arguments for and

---

[10] Andrea Fuller, *Effort to Replace Federal Driver's License Mandate Gains*, July 16, 2009, http://www.nytimes.com/2009/07/16/us/16identify.html (accessed July 16, 2009).

[11] Nikki Swartz, "REAL ID to Cost $11 Billion Plus," *Information Management Journal*, Jan/Feb 2007; 41, 1: 12.

against the RIA and other identification systems. This thesis argues that the use of biometric technology in driver licenses and identification cards systems would be a more effective counterterrorism technique than if the government continues to move forward with implementing the current RIA requirements.

C. METHODOLOGY

The methodology in this research is primarily analytic. The thesis includes an analysis of the arguments of the proponents and opponents of the RIA and national identification card standards. It also makes a comparative analysis of biometric identification through a review of various states' efforts for an Enhanced Driver's License (EDL) and federal agency programs, including US-VISIT, which require the collection and utilization of biometric information for national security purposes. Analysis of technical, statistical, polling information and data will result in a proposed recommendation to accomplish assured personal identification through the use of driver's licenses and identification cards.

D. ORGANIZATION OF THESIS

This thesis is organized into several chapters composed of background, technical, comparative analysis and recommendations. Chapter II provides an overview of the 9/11 Commission recommendations, the background on RIA legislation, REAL ID compliant card requirements and characteristics and financial costs. It also covers the opponent and proponent arguments regarding the RIA and the current status of the debate.

Chapter III provides the technical background on identification systems and biometrics, and an analysis of current technologies including limitations and their accuracy. The chapter explains how biometric technologies are used commercially and within the government, including Department of Defense (DoD) use of biometrics in Iraq and Afghanistan as a counterterrorism tool.

Chapter IV analyzes alternative courses of action including the use of the EDL. Elements such as implementation feasibility, cost, privacy protection, projected

effectiveness and benefits are analyzed. Chapter V gives a summary review and provides recommendations on how driver's licenses and identification cards can be improved.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. 9/11 COMMISSION RECOMMENDATION

The 9/11 Commission outlined how weaknesses and loopholes in immigration policy, lack of standards in the issuance of state driver's license and identification cards, and problems in border security enforcement allowed the 9/11 terrorists to easily travel to, from and within the United States prior to conducting the terrorist attacks.[12] The 9/11 Commission provided clear recommendations on the importance of resolving issues of personal identification within the United States:

> Secure identification should begin in the United States. The federal government should set standards for the issuance of birth certificates and sources of identification, such as driver licenses. Fraud in identification documents is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists.[13]

B. REAL ID ACT OF 2005 (RIA)

The 9/11 Commission Report was followed by a number of legislative bills including: the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), the Border Protection, Antiterrorism, Illegal Immigration Control Act of 2005, Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief (H.R. 1268), Comprehensive Immigration Reform Act of 2006, and Implementing the Recommendations of 9/11 Commission Act of 2007, all of which were intended to address some of the homeland defense and security problems identified by the 9/11 Commission.[14] In an effort to address the lack of standards with driver's licenses and

---

[12] Staff Report of the National Commission on Terrorist Attacks Upon the United States, *9/11 and Terrorist Travel*, Franklin, TN: Providence Publishing Corporation, 2004, 43–46.

[13] 9/11 Commission, *The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States*, Washington D.C. : http://www.9-11commission.gov/report/911Report.pdf, 2004, 390.

[14] Andorra Bruno, "Immigration Legislation and Issues in the 109th Congress," CRS Report to Congress, Updated December 7, 2006, 1–3.

identification cards the executive and legislative branches passed the REAL ID Act of 2005 (RIA). The RIA was passed as a supplement bill to the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief (H.R. 1268), and the way it became law is sometimes seen as more controversial than the legislation's content.

Even prior to the 9/11 Commission Report there was a growing consensus in Congress that something had to done to improve the identification system in the United States. In May 2002, Representative James Moran, Democrat from Virginia, introduced the Driver's License Modernization Act of 2002 (H.R. 4633).[15] Although H.R. 4633 never became law, it would have required each state: 1) to have a driver's license and identification card that contained biometric data and other security features, 2) link state motor vehicle databases electronically with the federal government, and 3) implement nationally-standardized procedures for accurately documenting the identity and residence of an individual before issuing a license or card.[16] Concerns over civil liberties, financial costs, states' rights, and that the legislation was a back door approach to combating illegal immigration led to the bill's defeat in Congress.

In 2004, Wisconsin Representative James Sensenbrenner, Republican and chair of the House Judiciary Committee, introduced the RIA as part of Section 7212 of the Intelligence Reform and Terrorism Prevention Act of 2004.[17] However, the RIA section of the legislation did not have support in the Senate. After the Senate threatened to kill the entire bill, the RIA was removed, but with agreement from House of Representative leadership that the RIA would be included in the next piece of legislation that both chambers were expected to pass.[18]

---

[15] , Anna Ya Ni and Alfred Tat-Kei Ho, "A Quiet Revolution or a Flashy Blip? The REAL ID Act and U.S. National Identification System Reform," *Public Administration Review*, Nov/Dec 2008; 68, 6:1071.

[16] Ibid., 1070.

[17] Ibid., 1071.

[18] Mary Curtius, *GOP Push for Immigration Curbs*, January 27, 2005. http://articles.latimes.com/2005/jan/27/nation/na-immig27 (accessed August 4, 2009).

On January 26, 2005, the RIA was re-introduced by Republican Representative James Sensenbrenner as H.R. 418; the bill was passed by the House, recommended to the Senate and subsequently reattached to a supplemental spending bill as H.R. 1268 without debate in the Senate.[19] The RIA became law as part of Public Law 109-13, Division B (H.R. 1268), as a supplemental appropriations bill.[20] The RIA included changes to asylum, outlined compliance requirements for state-issued licenses and identification cards, added limits on federal judicial review of removal of aliens, expanded exclusion and removal of terrorist suspects, and included funding to expedite the construction of border barriers and improve border infrastructure and technology integration.[21] The RIA includes the following driver's license and identification card compliance requirements: identity verification, document authentication, card security, security plans, one driver, one license, and federal official purpose requirement.[22]

1. Legislation

Under Public Law 109–13, Division B, the RIA is comprised of seven sections (Sections 201–207). Section 201 outlines the key definitions for the legislation. Section 202 establishes the minimum document requirements and minimum driver's license and identification card issuance standards for federal recognition. Section 203 amends 18 U.S.C. 1028(a) to establish a federal criminal penalty for persons who knowingly traffic in actual authentication features for use in fraudulent identification cards.[23] Section 204

---

[19] Martin W Ardis, *Real ID Act of 2005 and its Interpretation* (Hauppauge, NY: Nova Publishers, 2005), 3.

[20] Department of Homeland Security, *Public Law 109-13 109th Congress*, April 10, 2009. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_public_laws&docid=f:publ013.109 (accessed July 10, 2009).

[21] Andorra Bruno, "Immigration Legislation and Issues in the 109th Congress," CRS Report to Congress, Updated December 7, 2006, 1–4.

[22] Janice L. Kephart and Jena Baker McNeil, *The PASS ID Act: Rolling Back Security Standards for Driver's License*, Background Report on REAL ID Act and PASS ID Act, Washington D.C.: The Heritage Foundation, 2009, 3.

[23] Department of Homeland Security Notice of Proposed Rulemaking, "Minimum Standards for Driver's Licenses and Identification Cards Acceptable to Federal Agencies for Official Purposes," *DHS. REAL ID Act of 2005.* March 2007, http://www.dhs.gov/xlibrary/assets/nprm_realid.pdf (accessed July 26, 2009), 10.

authorizes the DHS Secretary to make grants to assist states with meeting the RIA standards and provides an authorization of appropriations for fiscal years 2005 through 2009.[24]

Section 205 grants authority to the DHS Secretary to issue regulations, set standards, and issue grants in consultation with the Secretary of Transportation and the states.[25] Section 206 repeals Section 7212 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458).[26] Section 7212, of Public Law 108–458, requires the federal government to establish a negotiated rule making committee of subject matter experts to propose workable driver's license standards.[27] Section 207, Limitation on Statutory Construction, limits the authority and specifies that nothing in the RIA affects the authorities or responsibilities of the Secretary of Transportation or the states under chapter 303 of title 49, United States Code.[28]

2. DHS Regulatory Review and Final Rulemaking

On March 9, 2007, DHS published a Notice of Proposed Rulemaking (NPRM) in the Federal Register requesting public comments on the RIA from states and citizens.[29] DHS received more than 21,000 comments to the NPRM; the comments are available for public view in the Federal Docket Management System at: http://www.regulations.gov.[30]

---

[24] Department of Homeland Security, *Public Law 109-13 109th Congress*, April 10, 2009. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_public_laws&docid=f:publ013.109 (accessed July 10, 2009).

[25] Ibid.

[26] Ibid.

[27] Senate Committee on Homeland Security & Governmental Affairs, *Web Cast of July 15, 2009 Identification Security: Reevaluating the REAL ID Act: (Senator Lieberman Opening Remarks, 26:05 Minute Mark)*, July 15, 2009.

[28] Department of Homeland Security, *Public Law 109-13 109th Congress*, April 10, 2009. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_public_laws&docid=f:publ013.109 (accessed July 10, 2009).

[29] National Archives and Records Administration, "Department of Homeland Security: 6 CFR Part 37, Docket No. DHS-2006-0030, Minimum Standards for Driver's Licenses and Identification Cards," *Federal Register*, March 2007, 2007, http://edocket.access.gpo.gov/2007/pdf/07-1009.pdf (accessed July 21, 2009).

[30] Department of Homeland Security, *REAL ID Act Regulatory Evaluation - Final Rulemaking*, Report Identification Number: 1601-AA37, Washington D.C.: DHS, January 17, 2008, 26.

DHS responded to all comments relating to the Regulatory Evaluation and subsequently issued the DHS Final Rulemaking Regulatory Evaluation for the RIA on January 17, 2008.

In accordance with the final ruling, RIA licenses and non-driver identity cards issued by states will be acceptable for official purposes. DHS refined and limited the definition of official purposes to those uses listed by Congress in the statute: boarding a federally-regulated commercial aircraft, accessing a federal facility, and entering nuclear power plants.[31] The RIA is not mandatory and permits states to continue to issue driver's licenses and identification cards that are not compliant with the RIA's requirements. However, if states want their residents to be able to use their driver's licenses to access federal facilities or get on a commercial airplane, the licenses must meet RIA requirements. The RIA requires DHS to determine whether a state has met RIA requirements based upon certifications submitted by each state to DHS. DHS must concur with compliance before a state-issued driver's license or identification card may be accepted by federal agencies for official purposes.[32]

The final rule sets four compliance dates related to the use of state driver's licenses and identification cards for official purposes:

1. May 11, 2008–federal government cannot accept state-issued driver licenses or identification cards for official purposes from states determined to be not in compliance unless an extension has been granted by DHS (DHS granted extensions to all 56 jurisdictions in 2008).[33]
2. January 1, 2010–the initial extension will terminate unless states are granted a second extension and meet certain RIA benchmarks. REAL ID

[31]Department of Homeland Security, *REAL ID Act Regulatory Evaluation - Final Rulemaking*, Report Identification Number: 1601-AA37, Washington D.C.: DHS, January 17, 2008, 35–36.

[32] Department of Homeland Security Notice of Proposed Rulemaking, "Minimum Standards for Driver's Licenses and Identification Cards Acceptable to Federal Agencies for Official Purposes," *DHS. REAL ID Act of 2005*, March 2007, http://www.dhs.gov/xlibrary/assets/nprm_realid.pdf (accessed July 26, 2009), 10.

[33] Department of Homeland Security, *REAL ID: States Granted Extensions*, November 10, 2008. http://www.dhs.gov/files/programs/gc_1204567770971.shtm#3 (accessed June 21, 2009).

cards from states granted a second extension and in material compliance with the rule will be accepted for official purposes (Reference Appendix: REAL ID Act Material Compliance Checklist for a complete listing of material compliance requirements).

3. December 1, 2014–only REAL ID cards will be accepted from individuals born on or after December 1, 1964, for official purposes.
4. December 1, 2017–Federal agencies will only accept REAL ID driver's license or identification cards for official purposes.[34]

3. Driver's License and Identification Card Standards

Section 202 of the RIA established the information and features that must appear on official driver's licenses or identification cards. REAL ID-compliant driver's licenses and identification cards must include the following components on the front of the card: full legal name, date of birth, gender (as determined by the state), unique driver's license or identification card number, address of principal residence, signature and a full facial digital photograph.[35] Individuals unable to sign their names are authorized to use the Latin alphabet as an alternative to the signature.[36]

Section 202 requires each person applying for a driver's license or identification card to submit to a mandatory facial image capture.[37] The digital photograph may be in black and white or color, and states must take the photograph at the beginning of the application process in order to deter applicants from presenting fraudulent documents, and "shopping" Department of Motor Vehicle (DMV) offices after being denied by

---

[34] Department of Homeland Security, *REAL ID Act Regulatory Evaluation - Final Rulemaking*, Report Identification Number: 1601-AA37, Washington D.C.: DHS, January 17, 2008, 36.

[35] Department of Homeland Security, "Final Rule: Minimum Standards for Driver's Licenses and Identifcation Cards Acceptable by Federal Agencies for Official Purposes," *Federal Register, Volume 73, Number 19*, January 28, 2008, http://edocket.access.gpo.gov/2008/08-140.htm (accessed July 1, 2009).

[36] Ibid.

[37] Department of Homeland Security Notice of Proposed Rulemaking, "Minimum Standards for Driver's Licenses and Identification Cards Acceptable to Federal Agencies for Official Purposes," *DHS. REAL ID Act of 2005*, March 2007, http://www.dhs.gov/xlibrary/assets/nprm_realid.pdf (accessed July 26, 2009), 67.

another DMV office in the same jurisdiction.[38] Individuals denied a REAL ID card will have their photograph stored for a period of five years, regardless of the reason that the state denies the application.[39] Digital photographs taken must comply with current International Civil Aviation Organization (ICAO) 9303 standards.[40]

Many states use a composite card stock material in driver's licenses and identification cards, often Teslin with a laminate overlay, which is vulnerable to counterfeit with modern copiers, scanners and printing equipment.[41] To prevent counterfeiting and altering of cards that use REAL ID's to create fraudulent documents, Section 37.15 of the RIA final ruling establishes anti-counterfeiting benchmarks for states requiring at least three levels of integrated security features.[42] The three levels of integrated security card features required for REAL IDs include: 1) Level 1–overt features visually or tactilely apparent by cursory examination without the use of aids, 2) Level 2–a feature detected by inspection through the use of basic tools or instruments, and 3) Level 3–covert feature detectable only through the use of forensic inspectors and the use of advanced tools and equipment.[43] In 2008, DHS determined that it would be in the best interest of the nation's security for states to place a security marking on the REAL ID-compliant driver's licenses and identification cards to allow federal agencies to easily distinguish between REAL ID-compliant cards and non-compliant cards.[44]

---

[38] Department of Homeland Security, "Final Rule: Minimum Standards for Driver's Licenses and Identifcation Cards Acceptable by Federal Agencies for Official Purposes," *Federal Register, Volume 73, Number 19,* January 28, 2008, http://edocket.access.gpo.gov/2008/08-140.htm (accessed July 1, 2009).

[39] Ibid.

[40] The relevant ICAO standard is ICAO 9303 Part 1 Vol. 2, specifically ISO/IEC 19794-5 - Information technology - Biometric data interchange formats - Part 5: Face image data, which is incorporated into ICAO 9303.

[41] Department of Homeland Security, *REAL ID Act Regulatory Evaluation - Final Rulemaking,* Report Identification Number: 1601-AA37, Washington D.C.: DHS, January 17, 2008, 30.

[42] Department of Homeland Security, "Final Rule: Minimum Standards for Driver's Licenses and Identifcation Cards Acceptable by Federal Agencies for Official Purposes," *Federal Register, Volume 73, Number 19,* January 28, 2008, http://edocket.access.gpo.gov/2008/08-140.htm (accessed July 1, 2009).

[43] Department of Homeland Security, "Final Rule: Minimum Standards for Driver's Licenses and Identifcation Cards Acceptable by Federal Agencies for Official Purposes," *Federal Register, Volume 73, Number 19,* January 28, 2008, http://edocket.access.gpo.gov/2008/08-140.htm (accessed July 1, 2009).

[44] Ibid.

The RIA requires states to incorporate machine readable technology, including a 2-dimensional (2-D) barcode on REAL ID driver's licenses or identification cards using the PDF-417 standard. PDF-417 is the endorsed standard by the International Organization for Standardization (ISO).[45] The 2-D barcode must include ten pieces of information: 1) expiration date, 2) full legal name, 3) date of transaction, 4) date of birth, 5) gender, 6) address, 7) unique driver's license or identification card number, 8) card design revision date, indicating the most recent change or modification to the visible format of the driver's license or identification card, 9) inventory control number of the physical document, and 10) state or territory of issuance.[46]

4. Financial Costs

Cost estimates to implement the requirements outlined in the RIA have ranged from $4 billion to in excess of $23 billion. Initially, DHS estimated the cost of implementing the RIA to be $23.1 billion over ten years, of which $10 billion to $14 billion would be funded by the states.[47] On January 17, 2008, DHS revised the RIA cost estimates in the RIA Regulatory Evaluation Final Rulemaking, reducing the overall cost estimate to $9.9 billion over 11 years, of which $3.97 billion would be required from the states.[48] The revised lower cost estimate is based on the DHS assumption that seventy-five percent of the nation's drivers will seek a REAL ID.[49] The assumption is based on the DHS analysis that: 1) a number of states will not require that all residents seeking driver's licenses and identification cards obtain a REAL ID, 2) 25 percent of the

---

[45] Department of Homeland Security, *REAL ID Act Regulatory Evaluation - Final Rulemaking*, Report Identification Number: 1601-AA37, Washington D.C.: DHS, January 17, 2008, 44.

[46] Department of Homeland Security, *REAL ID Act Regulatory Evaluation - Final Rulemaking*, Report Identification Number: 1601-AA37, Washington D.C.: DHS, January 17, 2008, 45.

[47] Senate Committee on Homeland Security and Governmental Affairs, *Impact of Implementation: A Review of the REAL ID Act and the Western Hemisphere Travel Initiative: Costs and Privacy Concerns*, April 29, 2008, 360.
http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Detail&HearingID=c8bd6312-5714-4a1c-8f25-eef90c611a44 (accessed July 10, 2009).

[48] Department of Homeland Security, *REAL ID Act Regulatory Evaluation - Final Rulemaking*, Report Identification Number: 1601-AA37, Washington D.C.: DHS, January 17, 2008, 9.

[49] Ibid., 2–3.

population already holds a valid passport, and a percentage of this population may not obtain a REAL ID, and 3) 20 percent of the population has never flown on a commercial airplane and 47 percent flies rarely; DHS assumes that only a percentage of this group will obtain a REAL ID.[50]

DHS estimates the four largest cost areas include: 1) opportunity costs to applicants ($5.2 billion), 2) maintaining the necessary data and interconnectivity ($1.5 billion), 3) customer service ($970 million), and 4) card production and issuance ($953 million).[51] Opportunity costs comprise the cost for individuals to obtain source documents, applications and visiting DMVs. Data and interconnectivity costs are the costs to the states for data systems and information technology. Customer service costs comprise the transaction costs to the state DMVs due to the increased number of customers acquiring REAL IDs. The card production and issuance costs are the costs to upgrade state driver's licenses and identification cards to meet the minimum REAL ID card standards.

Table 1 includes a complete breakdown of estimated costs as provided by DHS. Table 1 estimates are based on 477.1 million card issuances over 11 years of the analysis, with the average cost to the states per issuance being $8.31.[52] Individuals incur the largest share of the costs, with more than 58 percent of the costs associated with preparing applications, obtaining necessary documents, or visiting motor vehicle offices.[53]

---

[50] Department of Homeland Security, *REAL ID Act Regulatory Evaluation - Final Rulemaking*, Report Identification Number: 1601-AA37, Washington D.C.: DHS, January 17, 2008, 2–3.

[51] Ibid., 10.

[52] Ibid., 8–10.

[53] Department of Homeland Security, *REAL ID Act Regulatory Evaluation - Final Rulemaking*, Report Identification Number: 1601-AA37, Washington D.C.: DHS, January 17, 2008, 8–10

Estimated Costs (11 years)	$ million (2006 dollars)	% Total
Costs to States	**3,965**	**39.9%**
Customer Service	970	9.8%
Card Production	953	9.6%
Data Systems & Information Technology	1,529	15.4%
Security & Information Awareness	490	4.9%
Data Verification	8	0.1%
Certification Processes	16	0.2%
Costs to Individuals	**5,792**	**58.3%**
Opportunity Costs	5,215	52.5%
Application Preparation (125.8 million hours)	3,327	33.5%
Obtain Birth Certificate (20.1 million hours)	530	5.3%
Obtain Social Security Card (1.6 million hours)	44	0.4%
DMV Visits (49.8 million hours)	1,315	13.2%
Expenditures: Obtain Birth Certificate	577	5.8%
Costs to Private Sector	9	0.1%
Costs to Federal Government	171	1.7%
Social Security card issuance	50	0.5%
Data Verification–SAVE	14	0.1%
Data Systems & Information Technology	82	0.8%
Certification & training	25	0.3%
Total Costs	**9,939**	**100%**

Table 1. Estimated Marginal Economic Cost of RIA (From Final Ruling, 9)

C. NATIONAL IDENTIFICATION CARD DEBATE

For the purposes of this thesis, a national identification system is defined as a system where the federal government, in coordination with the states, has established compulsory requirements and standards for state-issued driver's licenses and identification cards. The cards themselves can be issued by the states. Like many policies, the public debate between proponents and opponents of identification system

changes, the RIA, and national identification cards reflects tensions between certain core values: federal power versus state and local authority, equal protection versus state sovereignty, individual privacy versus law for governing the public, convenience versus privacy, and national security versus economy.[54] Since the RIA became law, there have been many editorials in newspapers and magazines and postings on Internet blogs and citizen organization Web sites outlining the proponent and opponent arguments. Some of the important questions debated include: 1) does the public support changes to identification systems? 2) what biometric data should be required on driver's licenses and identification cards? 3) will changing identification systems improve national security? 4) is there a cost benefit? 5) how will the changes be paid for? and 6) how does creating a national standard for driver's licenses and identification cards affect individual privacy and civil liberties? This section will examine public opinion on the RIA and national identification standards, and the proponent and opponent arguments.

1. Public Opinion on National Identification Card Standards

No matter what identification card standards and policies are implemented to address the terrorist threat, in order for government resources to be allocated and implementation to be successful, public support of the counterterrorism measure is important. Polling data indicates public awareness of the terrorist threat and support for national identification cards as a counterterrorism measure. According to several polls conducted by the Pew Research Center, the American public's assessment of terrorists' abilities to launch another major attack against the United States have remained relatively stable since 9/11: In 2002, 61 percent of the American public believed the ability of the terrorists to launch an attack was about the same or greater than the 9/11 attacks, and in February 2009, 61 percent agreed.[55]

---

[54] Anna Ya Ni and Alfred Tat-Kei Ho, "A Quiet Revolution or a Flashy Blip? The REAL ID Act and U.S. National Identification System Reform," *Public Administration Review*, Nov/Dec 2008; 68, 6: 1074.

[55] Pew Research Center, *No Change in Views of Torture, Warrantless Wiretaps*, February 2009 News Release–Latest Poll, Washingt D.C.: Peoples Press, 2009, 2–3.

Immediately after 9/11, 70 percent of the American public supported counterterrorism measures that would require citizens to carry a national identity card at all times and to show it to a police officer upon request.[56] In 2004, 56 percent supported the idea, but the drop did not reflect any break along partisan or ideological lines.[57] A poll conducted in 2006 revealed that 57 percent supported requiring a national identification card as a counterterrorism policy.[58]

2. Proponent Arguments

The driver's license is the most common form of identification used in the United States today, accepted for everything from opening a bank account to boarding a plane to picking up movie tickets with a credit card.[59] To proponents, securing an already widely used credential and making it more difficult for criminals and terrorists to acquire them makes sense.[60] Proponents of the RIA argue that,

> The 9/11 hijackers obtained 30 different driver's licenses and identification cards and used 364 aliases, [and] for an extra $8 per license REAL ID will give law enforcement and security officials a powerful advantage against falsified documents, and it will bring some peace of mind to citizens wanting to protect their identity from theft by a criminal or illegal alien.[61]

This section examines the proponent arguments that the RIA and national identification card standards will improve security, are cost beneficial, and reduce counterfeiting and identity theft.

---

[56] Pew Research Center, *Evenly Divided and Increasingly Polarized*, Political Landscape Poll, Washington D.C.: People Press, 2004, 73–74.

[57] Ibid., 73.

[58] Pew Research Center, *News Release - Latest Poll*, December 2006 Poll Data, Washington D.C. : Peoples Press, 2006, 9–10.

[59] Senate Committee on Homeland Security and Governmental Affairs, *Impact of Implementation: A Review of the REAL ID Act and the Western Hemisphere Travel Initiative Testimony from Janice Kephert, Former Counsel 9/11 Commission*, April 29, 2008. http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Detail&HearingID=c8bd6312-5714-4a1c-8f25-eef90c611a44 (accessed April 10, 2009).

[60] Ibid.

[61] Matt Sundeen, "The REAL ID Rebellion " *State Legislatures*, Mar 2008; 34, 3: 26.

a. Improved Security

The primary benefit of the RIA and establishing national standards for driver's licenses and identification cards, advocates argue, is to improve national security by reducing the vulnerability of federal buildings, aircraft and nuclear facilities to criminal or terrorist activity.[62] The author of the RIA, Representative James Sensenbrenner (R-Wisconsin) stated,

> REAL ID is a necessary program for keeping America safe, it is the will of the Congress and also a recommendation of the 9/11 Commission . . . repealing this important recommendation and substituting it with a weaker, less safe program provides terrorists with too many avenues to attack.[63]

Sensenbrenner continued, "Without being able to change their identity terrorists are easier to detect and their plans easier for law enforcement to thwart–making everyone safer."[64]

The proponents are not necessarily a homogenous group. Some proponents of the RIA and national identification card standards argue that the RIA is a positive step forward in securing identification systems and improving national security, but the federal government should encourage the inclusion of additional biometric indicators in identification cards and use biometric technologies to provide a better defensive mechanism against terrorists. United States Congressman Mark Souder, Republican leader of the Homeland Security Subcommittee on Border, Maritime, and Global Counterterrorism, is a proponent of the RIA and national identification card standards, but argues that the federal government should encourage states to incorporate biometric indicators in REAL ID-compliant driver licenses. Representative Souder states:

---

[62] Department of Homeland Security, "Final Rule: Minimum Standards for Driver's Licenses and Identifcation Cards Acceptable by Federal Agencies for Official Purposes," *Federal Register, Volume 73, Number 19,* January 28, 2008, http://edocket.access.gpo.gov/2008/08-140.htm (accessed July 1, 2009).

[63] CNN Washington D.C. Office. *Homeland Security Chief seeks to repeal REAL ID Act,* April 22, 2009, http://www.cnn.com/2009/POLITICS/04/22/real.ID.debate/ (accessed April 23, 2009).

[64] Charlie Sykes, *Senenbrenner Smacks A Clueless Napalitano,* April 22, 2009. http://www.620wtmj.com/shows/charliesykes/43478517.html (accessed May 10, 2009).

> Fundamentally, our homeland security is tied to the integrity of everyone's identification card. We can improve intelligence-sharing among federal agencies, we can construct physical and electronic fences along the border, and we can scan incoming cargo at our ports—but if we can't verify the identity of someone trying to enter the United States (or the identity of someone who is already here) then we render much of our defenses impotent. I believe that Congress should consider legislation providing financial incentives or direct funding to states that include biometrics in their REAL ID Act-compliant driver licenses. By putting to work everyone's individual uniqueness, we can improve all of our security.[65]

Proponents of the RIA note that the combination of implementing the requirements of the RIA and the use of enhanced biometric technologies are having a positive impact in helping to identify and prosecute criminals in some states. Indiana is using enhanced biometric technology including facial recognition software to find identity thieves and criminals. In November 2008, the Indiana Bureau of Motor Vehicles (BMV) activated facial recognition technology in all BMV license branches to compare new photographs with the 6 million photographs in the BMV photo database. Using the facial recognition technology to examine the 6 million photos in the database, the Indiana BMV identifies on average six new cases of possible identity theft per day. Indiana cites the capture and imprisonment of David Grice who held five fraudulent identities, and William Sherman Smith who had 149 different driver's licenses issued using the same photo and different names as major successes for the program.[66]

b. Cost Benefit of Preventing a Terrorist Attack

The immediate economic impact of the 9/11 attacks on the United States is estimated at between $55.8 billion and $63.9 billion just from the physical destruction, seven-day shutdown of airline system and lost New York City gross city product in the

---

[65] Mark Souder, *Why we need ID's with Biometric Indicators*, January 10, 2008. http://souder.house.gov/index.cfm?FuseAction=NewsCenter.Articles&ContentRecord_id=69f68198-19b9-b4b1-1237-e37db00e6ddd&Region_id=&Issue_id=67cc589f-7e9c-9af9-7359-9a4ae482194b (accessed July 3, 2009).

[66] Indiana Bureau of Motor Vehicles, *Identity Thieves Caught By DMV*, August 9, 2009. http://www.in.gov/bmv/5168.htm (accessed August 9, 2009).

three months after the 9/11 attacks.[67] The economic impacts of another terrorist attack of the magnitude of 9/11 to the United States over two years are estimated at $374.7 billion.[68]

To assess the cost benefit of the RIA, DHS conducted an analysis based on several different methodologies including: 1) assessing the discounted cost of a single attack comparable to the 9/11 attacks taking place sometime over the next eleven years, 2) RIA having an impact on the annual probability of the United States experiencing a 9/11 type attack (involving air transportation) in the eleven years following the issuance of the rule, and 3) the impact if the RIA were to prevent an incident that was half the magnitude in terms of the direct short-term impact of the 9/11 attacks (50 percent of the $63.9 billion or $32 billion).[69]

Results of the DHS analysis indicate: 1) based on the first methodology, if the RIA requirements lowered by 0.25% per year the annual probability of a terrorist attack that caused both immediate and longer run impacts of $374.7 billion, the quantified benefits would be positive, 2) using methodology number two, the effects of the RIA are difficult to quantify and, 3) under the third analysis, if the RIA requirements lowered the annual probability of a terrorist attack by 2.9 percent per year the quantified net cost benefits of the RIA regulation would be positive.[70]

c. Counterfeiting and Identity Theft Prevention

A goal of the RIA is to help curtail identity theft and counterfeiting of driver's licenses and identification cards. In the pre-9/11 environment people thought of teenagers using fake identification cards for buying beer or cigarettes or gaining access to

[67] Department of Homeland Security, *REAL ID Act Regulatory Evaluation - Final Rulemaking*, Report Identification Number: 1601-AA37, Washington D.C.: DHS, January 17, 2008, 134.

[68] Ibid., 133.

[69] Ibid., 149–150.

[70] Ibid., 150.

bars, but post 9/11 the implications are different.[71] In the post-9/11 environment counterfeiting of driver's licenses is not just about buying cigarettes and beer. By obtaining counterfeit identification cards criminals and terrorists can open banking accounts, drive a vehicle, board commercial aircraft or acquire an apartment. Counterfeiting of non-REAL ID compliant cards is relatively easy and often big business for criminals. According to Major David Myers, of the Florida Alcoholic Beverages and Tobacco Division, "It's not unusual to bust a counterfeiter who has made over 10,000 falsified documents."[72] REAL ID's will incorporate at least three levels of security features in driver's licenses and identification cards, making it more difficult and costly for criminals and terrorists to create counterfeit identification cards.

DHS conducted an analysis of identity theft complaints reported by the Federal Trade Commission (FTC) in 2005. Presentation of a driver's license accounted for 28% of all reported incidents.[73] The types of identity theft requiring presentation of a driver's license included in the analysis are: medical fraud, evasion of legal sanctions, bank fraud (existing new accounts), employment fraud, house/apartment/rental property fraud and insurance fraud.[74] DHS estimated that if the RIA reduced the successful commission of driver's license related identity theft by 10 percent, a benefit of $0.6 billion would be attained over five years.

An analysis of the 2008 FTC data on identity theft and fraud indicates there may be even more savings than estimated in 2005 by implementing the RIA or equivalent identification card standards. According to the FTC, from January through December 2008 identity theft (26%) and fraud (52%) comprised 78% of the 1.2 million

[71] Warren St. John, *In the ID Wars, the Fakes Gain,* March 6, 2005. http://www.nytimes.com/2005/03/06/fashion/06fake.html?_r=1&pagewanted=print&position= (accessed July 14, 2009).

[72] Ibid.

[73] Department of Homeland Security, *REAL ID Act Regulatory Evaluation - Final Rulemaking,* Report Identification Number: 1601-AA37, Washington D.C.: DHS, January 17, 2008, 146.

[74] Ibid.

consumer complaints received.[75] In 2008, medical fraud, evasion of legal sanctions, bank fraud (existing and new accounts), employment fraud, house/apartment/rental property fraud and insurance fraud together accounted for 31.4% of all reported incidents, which is a 3% increase over 2005.[76] An estimate of the resource cost to households is not available from DHS for 2008, but applying the same estimate of a 10% benefit which was utilized by DHS in the initial analysis would result in a substantial savings to consumers equal to or higher than the DHS estimate based on 2005 FTC data.

d. Ancillary Benefits

There are several possible ancillary benefits to the RIA and establishing national identification card standards that are not necessarily quantifiable but include reducing: fraudulent access to public subsidies from government programs such as Medicaid, Medicare and in-state tuition rates by non-residence, the hiring of illegal immigrants, unlawful employment of convicted criminals, unlawful access to firearms, and voter fraud.[77]

3. Opponent Arguments

This section addresses the opponent arguments against the RIA and national identification card standards. Key areas of concern include impact to civil liberties, vulnerability to criminal activity, funding, impact to state rights and the lack of debate by the Senate prior to being passed. Some opponents of the RIA also argue that they do not necessarily oppose the concept of national identification card standards, but they have concerns over how the RIA was enacted and how DHS is implementing the legislation.

---

[75] Federal Trade Commission, "Consumer Sentinel Data Book January - December 2008." *www.ftc.gov*. February 26, 2009. http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf (accessed July 14, 2009), 3.

[76] Ibid., 12.

[77] Department of Homeland Security, *REAL ID Act Regulatory Evaluation - Final Rulemaking*, Report Identification Number: 1601-AA37, Washington D.C.: DHS, January 17, 2008, 148–149.

a. Civil Liberty and Privacy Concerns

There are concerns that implementing the RIA will infringe on individual privacy and security. One question is: If the government stores driver's license and identification card data in a central database or an integrated state database system, who will have access to the information and when could it be accessed? Many privacy advocates are concerned about the collection and retention of data in large state databases will lead to an integrated national database on all 245 million driver's license and identification card holders.[78] The creation of a central repository would provide government agencies a valuable tool to conduct surveillance on citizens and legal residents or make large millions of individual personal records vulnerable to theft.[79] Anne Collins, the former Registrar of Motor Vehicles for the Commonwealth of Massachusetts, said in testimony to the DHS Data Privacy and Integrity Advisory Committee, "If you build it they will come."[80] Jim Harper, Director of Information Policy Studies for the Cato Institute continued, "Massed personal information will be an irresistible attraction to DHS and many other governmental entities who will dip into data about us for an endless variety of purposes."[81] Large-scale data breaches have occurred in state DMVs across the country. In 2005, the Oregon DMV lost a half million records, and as databases are linked under RIA, opponents worry the breaches will only grow in scale.[82]

The Electronic Privacy Information Center (EPIC) states that while the RIA creates a national identification system the federal government has punted the issue

---

[78] Nikki Swartz, "REAL ID to Cost $11 Billion Plus," *Information Management Journal*, Jan/Feb 2007; 41, 1: 12.

[79] Anna Ya Ni and Alfred Tat-Kei Ho, "A Quiet Revolution or a Flashy Blip? The REAL ID Act and U.S. National Identification System Reform," *Public Administration Review*, Nov/Dec 2008; 68, 6, 1067.

[80] Jim Harper, "Understanding the Realities of REAL ID," *Vital Speeches of the Day*, May 2007: 208–212, 210.

[81] Ibid., 210.

[82] Electronic Privacy Information Center, "REAL ID Implementation Review Few Benefits, Staggering Costs," *epic.org.*, May 2008. http://epic.org/privacy/id-cards/ (accessed April 19, 2009), 20.

of privacy protection to the states.[83] EPIC continues, "The RIA does not include statutory language authorizing DHS to prescribe privacy requirements for the state controlled databases or data exchanges necessary to implement the RIA … [therefore] the Privacy Act of 1974 must be mandated in the RIA implementation regulations in order for DHS to fulfill its obligations."[84]

b. Identification Systems Vulnerable to Criminal Activity

Critics charge that if states implement the RIA using the current requirements, potential terrorists would be able to exploit identification card system vulnerabilities when planning, traveling and conducting terrorist attacks within the United States just as Al Qaeda did for the 9/11 terrorist attacks. Regardless of the improvements made to identification systems the systems are still vulnerable to criminal activity from a small minority of DMV employees and others with access to personal information contained in the databases. Bruce Schneier, a prominent security technologist, argues,

> REAL ID will not prevent people from getting legitimate identification cards with fraudulent names . . . three of the 9/11 terrorists had valid Virginia driver's licenses in fake names after bribing a DMV employee . . . any identification system involves people, fallible people who make regular mistakes.[85]

In July 2009, the Los Angeles Police Department, FBI, and district attorney's office tracked Shamsha Laiwalla, a Pakistan native in Los Angeles, and 13 accomplices who allegedly paid DMV workers in several states to provide fraudulent documents including driver's licenses.[86] One of Laiwalla's contacts altered DMV records for members of a criminal organization that dealt drugs and sold counterfeit

---

[83] Electronic Privacy Information Center, "REAL ID Implementation Review Few Benefits, Staggering Costs," *epic.org.*, May 2008, http://epic.org/privacy/id-cards/ (accessed April 19, 2009), 11.

[84] Ibid., 20.

[85] Bruce Schneier, *Will REAL ID Actually Make Use Safer? An Examination of Privacy and Civil Liberty Concerns*, May 8, 2007, http://www.schneier.com/testimony-realid.html (accessed May 21, 2009).

[86] Joel Rubin, *Counter-terrorism Investigators Find Alleged Identity Theft Ring.* July 26 , 2009. http://www.latimes.com/entertainment/news/music/la-me-fraud26-2009jul26,0,7924251.story?track=rss (accessed July 27, 2009).

goods; the money from the criminal enterprise is suspected of helping to fund Hezbollah, a militant Shiite Muslim group.[87] George Huber, commander of the California DMV's internal affairs branch, acknowledges the challenge stating, "There is always going to be a criminal element outside that is going to be looking to exploit weaknesses in our system … our employees don't get paid very much [and] the temptation is always there."[88]

c. Unfunded Mandate to States

In 2008, the DHS cost estimate for the RIA was $9.9 billion over eleven years, but many governors and state representatives believe the DHS estimate is low. In 2006, the National Governors Association (NGA), National Conference of State Legislatures (NCSL) and the American Association of Motor Vehicle Administrators (AAMVA) conducted a nationwide survey of state motor vehicle agencies to understand the fiscal and operational impact of the RIA. Based on the results of the survey the NGA, NCSL and AAMVA concluded that RIA will cost more than $11 billion over five years.[89]

In describing the impact of the RIA on states the NGA described the RIA as unrealistic and "an unfunded mandate of $11 billion over five years that its members cannot afford."[90] Janet Napolitano, the current Secretary of DHS, while governor of Arizona, "signed [a bill], barring Arizona's compliance with the Real ID program, …, she called it an unfunded federal mandate that would stick states such as Arizona with a multibillion-dollar bill for the cost to develop and implement."[91]

---

[87] Joel Rubin, *Counter-terrorism Investigators Find Alleged Identity Theft Ring*, July 26 , 2009. http://www.latimes.com/entertainment/news/music/la-me-fraud26-2009jul26,0,7924251.story?track=rss (accessed July 27, 2009).

[88] Ibid.

[89] National Governors Association, National Conference of State Legislatures, American Association of Motor Vehicle Administrators, *The REAL ID Act: Nationl Impact Analysis*, Washington D.C.: AAMVA, September 2006, 2.

[90] Audrey Hudson, "Napolitano Debates Real ID," *The Washington Times*, February 20, 2009. http://www.washingtontimes.com/news/2009/feb/20/napolitano-debates-real-id/ (accessed February 23, 2009).

[91] Benson, Matthew, "Napolitano: Real ID a no-go in Arizona," *Arizona Central News*, June 18, 2008. http://www.azcentral.com/news/articles/2008/06/18/20080618real-id0618.html (accessed February 23, 2009).

d. Federal Power vs. State and Local Authority

The Tenth Amendment of the United States Constitution states: *The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people*.[92] State rights proponents argue that the RIA infringes upon states rights established by the Tenth Amendment, arguing that the RIA is another example that the balance of power between the states and the federal government is out of alignment.[93]

Citizen opponents of the federal government imposing national identification standards on states are also actively engaged in the debate. Michael Boldin, a 36-year-old Web marketer, founded the Web site TenthAmendmentCenter.com, which has grown to 20,000 viewers per day, after watching the Maine State Legislature fight DHS on the RIA.[94] Boldin states, "Maine resisted, the government backed off, and soon all of these other states were doing the same thing."[95] Since 2007, 21 states have passed measures either prohibiting state compliance with the RIA or have urged Congress to amend or repeal the Act.[96]

e. RIA Legislation Passed without Debate

Not all opponents of the RIA are against the concept of implementing national standards for driver's licenses and identification cards. Some opponents of the RIA argue that the RIA was rushed through without adequate debate and there should be further national discussion on how best to address identification problems. Because the RIA was moved through the legislative approval process quickly as part of a supplemental bill, real debate over national identification did not take place until after

---

[92] Tenth Amendment, *The Charters of Freedom: Bill of Rights*, August 11, 2009. http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html (accessed August 11, 2009)

[93] James Osborne, *10th Amendment Movement Aims to Give Power Back to States*, May 26, 2009. http://www.foxnews.com/politics/2009/05/26/tenth-amendment-movement-aims-power-states/ (accessed July 10, 2009).

[94] Ibid.

[95] Ibid.

[96] Matt Sundeen, "The REAL ID Rebellion," *State Legislatures*, March 2008; 34, 3: 26.

RIA was signed into law.[97] According to a public policy assessment of the RIA conducted by Anna Ya-Ni and Alfred Tat-Kei Ho, "Changes which have significant and long lasting effects should only occur through a democratic, accountable and transparent process . . . and there are serious doubts as to whether the RIA could have met this criterion."[98]

D. CURRENT STATUS

This section will examine the current status of the RIA and recent developments pertaining to national identification card standards. On July 15, 2009, the Senate Homeland Security and Government Affairs Committee (Homeland Security Committee) conducted a hearing to re-evaluate the RIA and debate the elements of new legislation is entitled Providing Additional Security in States Identification (PASS ID) Act (S. 1261).[99] Senator Joseph Lieberman, Independent of Connecticut and chairman of the Homeland Security Committee, opened the hearings by stating;

> I regret to say that I'm not surprised we are here today, when Congress adopted the RIA as an amendment to a supplemental appropriations bill—without hearings of any kind or formal public vetting—we replaced a process for developing federal identification requirements that Senator Collins and I had made part of the Intelligence Reform and Terrorism Act of 2004, the so-called 9/11 Commission legislation.[100]

Key members of the 9/11 Commission have also weighed in on the lack of progress which has been made since the 9/11 Commission Report was published. In July 2009, the bipartisan National Security Preparedness Group (NSPG) was formed, which is headed by 9/11 Commission co-chairs Thomas Kean and Lee Hamilton. NSPG gathered to pressure the government to act on the 9/11 Commission's unfinished business

---

[97] Anna Ya Ni and Alfred Tat-Kei Ho, "A Quiet Revolution or a Flashy Blip? The REAL ID Act and U.S. National Identification System Reform," *Public Administration Review*, Nov/Dec 2008; 68, 6: 1071.

[98] Ibid., 1074.

[99] Andrea Fuller, *Effort to Replace Federal Driver's License Mandate Gains*, July 16, 2009. http://www.nytimes.com/2009/07/16/us/16identify.html (accessed July 16, 2009).

[100] Senate Committee on Homeland Security & Governmental Affairs, *Web Cast of July 15, 2009 Identification Security: Reevaluating the REAL ID Act: (Senator Lieberman Opening Remarks, 25 Minute Mark)*, July 15, 2009.

including the failure to enforce national standards for state driver licenses and identification cards.[101] Thomas Kean stated, "I'm worried that 20 percent [of the recommendations] haven't been addressed, [and] I'm worried that among the 80 percent things aren't fully done."[102]

1. RIA

Many states have made progress and are working towards meeting the requirements established by the RIA. However, thirteen states have enacted laws prohibiting compliance with the RIA, and it is unlikely that the majority of states will meet the next milestone, which is the material compliance deadline. In March 2009, the DHS Inspector General (IG) outlined several areas of concern with the implementation of the RIA. The DHS IG reported that 95% of states stated that DHS grants are insufficient to mitigate RIA implementation, that DHS guidance to states is not being provided in a timely fashion, that 68% of states report that implementation is cost prohibitive, and that states may not meet the December 31, 2009, material compliance deadline.[103]

On July 15, 2009, in testimony before the Homeland Security Committee, DHS Secretary Napolitano stated; "from the perspective of DHS, the major problem is that it is producing very little progress in terms of securing driver's licenses …simply put, REAL ID is unrealistic."[104] Napolitano continued, "Today, this hefty burden is made even more onerous by the economic conditions that are constricting state budgets."[105] Representative Sensenbrenner, the sponsor of the RIA, argues; "to date, states have received approximately $130 million from the federal government towards RIA

---

[101] Jeanne Merserve and Mike Ahlers, *9/11 Commission Members Act to Finally Wrap it up*, July 25, 2009, http://www.cnn.com/2009/US/07/25/new.antiterror.group/index.html (accessed July 25, 2009).

[102] Ibid.

[103] Department of Homeland Security Office of the Inspector General, "Potentially High Costs and Insufficient Grant Funds Pose a Challenge to REAL ID Implementation," OIG-09-36, Washington D.C., March 2009, 11–21.

[104] Senate Committe on Homeland Security and Governmental Affairs, "DHS Secretary Janet Napolitano," *Hearings: Identification Security: Reevaluating REAL ID*, July 15, 2009. http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=3d9a52cd-c442-4dee-9a1f-b02ed3b38000 (accessed July 17, 2009).

[105] Ibid.

implementation, while additional funding will be needed to further implement the RIA, this program has a positive return on investment by eliminating waste and reducing fraud."[106] Although the debate continues over the RIA, because of lack of progress by states to complete the material compliance requirements, DHS and the legislative branches will have to determine whether to repeal the RIA or grant a second extension to allow states to meet the material compliance requirements outlined in the legislation.

2. PASS ID Act

There is legislative movement to replace the RIA with the PASS ID Act (S.1261). The components of the PASS ID Act were recently debated before the Senate Homeland Security Committee. In testimony, DHS Secretary Napolitano stated, "All in all, PASS ID is the fix for REAL ID that the nation needs, one that keeps strong security standards that are critical to our safety, but provides workable ways to achieve those standards."[107] Key differences between the RIA and initial PASS ID Act legislation include: RIA mandates electronic verification for validating the underlying the documents of a state issued driver's license while PASS ID allows states options to make these determinations, DHS projects lower potential costs to states, PASS ID could be completed faster than the RIA; if Congress passed PASS ID in October 2009 the states could complete enrollment by July 2016, and PASS ID would not require states to provide direct access to each other's driver's license databases.[108] In terms of the physical card characteristics, there have not been any major changes proposed which would change the requirements from those established in the RIA.

During the Homeland Security Committee hearings, several Senators expressed concerns with allowing states flexibility in verifying citizenship and with how the PASS

---

[106] Charlie Sykes, *Senenbrenner Smacks A Clueless Napalitano,* April 22, 2009. http://www.620wtmj.com/shows/charliesykes/43478517.html (accessed May 10, 2009).

[107] Ibid.

[108] Senate Committe on Homeland Security and Governmental Affairs, "DHS Secretary Janet Napolitano," *Hearings: Identification Security, Reevaluating REAL ID,* July 15, 2009. http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=3d9a52cd-c442-4dee-9a1f-b02ed3b38000 (accessed July 17, 2009).

ID Act might impact the Transportation Security Administration (TSA) responsibilities. Senator Lieberman requested additional discussions with DHS to resolve concerns prior to presenting the PASS ID Act for a committee vote. The issues of concern were resolved within two weeks. On July 29, 2009, the Senate Homeland Security Committee approved the PASS ID Act (S. 1261) by a unanimous vote after being amended to require: motor vehicle departments verify the authenticity of birth records prior to issuing driver's licenses, and TSA retains its current authority.[109]

Although the PASS ID Act legislation has passed through the Senate Homeland Security Committee there are still many unanswered questions pertaining to the impact to states, the financial costs and whether the PASS ID Act is an improvement over RIA. According to David Quan, the Director of Federal Relations for the National Governors Association, the implementation costs for PASS ID are estimated to be in the $2 billion range, although DHS and no states have conducted a comprehensive cost estimate.[110] Cost savings are projected to come from elimination of the RIA requirement for states to use electronic databases to verify U.S. passport information and savings from the development of new databases which would allow states to share driver's license and identification card information with each other. These databases do not exist or are not currently nationally deployed to DMVs.

Opponents of PASS ID argue that PASS ID is a watered down version of the RIA and it will make the U.S. less safe. Representative Sensenbrenner stated: "PASS ID is nothing but a smoke screen, allowing the Obama administration and DHS Secretary

---

[109] Senate Committee on Homeland Security & Governmental Affairs, *Secure Identification Fix Clears Committee*, July 29, 2009. http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord_id=c7f85c1e-5056-8059-76ef-4b4cb7649086&Region_id=&Issue_id=716b4c83-7747-4193-897b-632e5c281a91 (accessed July 30, 2009).

[110] Senate Committee on Homeland Security and Governmental Affairs, "David Quam, Director of Federal Relations, National Governors Association Opening Statement," *Hearings: Identification Security, Reevaluating REAL ID*, July 15, 2009. http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=3d9a52cd-c442-4dee-9a1f-b02ed3b38000 (accessed July 17, 2009).

Napolitano to turn back the clock to pre-9/11, while putting America at risk."[111] Sensenbrenner continued, "Legislation must allow states to cross check an ID and mandate rigorous identity checks."[112]

[111] Andrea Fuller, *Effort to Replace Federal Driver's License Mandate Gains.* July 16, 2009. http://www.nytimes.com/2009/07/16/us/16identify.html (accessed July 16, 2009).

[112] Ibid.

III. IDENTIFICATION TECHNOLOGIES AND USES

A. BIOMETRICS

Identification is the use of attributes to understand who a person is or refer to a person, and biometrics refers to measurable (anatomical or physiological) and behavioral characteristics such as fingerprint, facial or iris recognition, that can be used for automated recognition, and also verification or authentication of claimed identity.[113] "With the advent of biometrics, it is now possible to establish an identity based on who you are rather than by what you possess or what you remember."[114] Establishing that you are not someone—a negative claim to identity—can only be accomplished through biometrics.[115] The following sections examine the basic characteristics of a biometric system including an analysis of how individuals enroll, how biometric systems are utilized, some of the commonly used performance metrics which are used to evaluate system accuracy and a comparison of the most commonly used biometric systems.

1. Basic Biometric System

A biometric system is a pattern recognition system that acquires biometric data from an individual, extracts a feature set from the data, compares this feature set against the feature set stored in a database, and executes an action based on the result of the comparison.[116] Although there are many types of biometric systems, all biometric systems involve processes which can be divided into two stages: enrollment, and either verification or identification.[117] A generic example of the components of a biometric

---

[113] George W. Bush, *Biometrics for Identification and Screening to Enhance National Security/NSPD-59/HSPD-24,* Washington D.C. , June 5, 2008.

[114] Anil K Jain, Patrick Flynn, and Arun Abraham Ross, *Handbook of Biometrics,* New York: Springer, 2007, 2.

[115] Dr. James Wayman, *National Biometrics Test Center: Biometrics Publications,* 2000. http://www.engr.sjsu.edu/biometrics/publications_tech.html (accessed May 20, 2009).

[116] Anil K Jain, Patrick Flynn, and Arun Abraham Ross, *Handbook of Biometrics,* New York: Springer, 2007, 3.

[117] United States General Accounting Office (GAO), *Technology Assessment: Using Biometrics for Border Security,* Washington D.C.: GAO, November 2002, 40.

system can be viewed as a sensor module, a quality assessment and feature extraction module, a matching module and a database module.[118]

a. Enrollment

Biometric authentication involves the comparison of an enrolled biometric sample against a newly-captured biometric sample. The enrollment process involves presenting a biometric for capture to the sensor module, processing the information by a computer and storing the information in a database for a comparison. The quality assessment and feature extraction module assesses the sample, also referred to as the trial, collected by the sensor to determine if the sample is suitable for further processing. If the sample is not of high enough quality then the individual will be required to present the biometric again. Once the collected biometric feature set meets the biometric systems quality standard, the feature set is stored in a database. The collected biometric feature set is referred to as the template. The system database acts as the repository of the template along with other biographic information such as name, address and age which characterizes the identity of the individual.[119]

b. Verification

The biometric system can operate in either verification or identification mode. In verification mode, the biometric system authenticates an individual's claimed identity from their previously enrolled biometric template. In the verification based system, the individual who desires to be recognized claims an identity, usually a name or user name, or holds a smart card which is entered into the biometric system prior to presenting a biometric sample. Once the biometric sample is presented to the sensor, the biometric system conducts a one-to-one comparison against the biometric template to

[118] Anil K. Jain, Patrick Flynn, andArun Abraham Ross, *Handbook of Biometrics,* New York: Springer, 2007, 3.

[119] Ibid., 4–5.

determine whether the claim of identity is true or not.[120] The objective of the verification process, referred to as one-to-one matching, is to prevent multiple people from using the same identity.[121]

An example of a basic biometric system operating in verification mode is shown in Figure 1. An individual who is enrolled in the biometric system will have their biometric template stored in a database. During verification the individual will present their biometric which is captured, processed and then compared to the specific individual's stored biometric template. If the presented biometric sample matches the reference template, then the system will display a green light, otherwise a red light is displayed indicating a rejection of the individual.

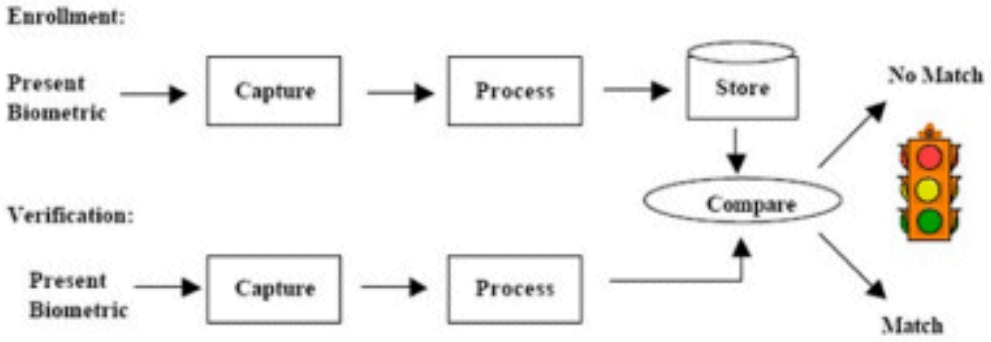

Figure 1. Basic Biometric System in Verification Mode[122]

c. Identification

In identification mode, often described as one-to-many matching, instead of locating and comparing a person's reference template against the presented biometric, the biometric system identifies a person from the entire enrolled population by searching a database for a match based solely on the biometric.[123] Biometric systems operating in

---

[120] Anil K. Jain, Patrick Flynn, andArun Abraham Ross, *Handbook of Biometrics*, New York: Springer, 2007, 6.

[121] GlobalSecurity.org., *Homeland Security: Biometrics*, June 2009. http://www.globalsecurity.org/security/systems/biometrics.htm (accessed June 1, 2009).

[122] Ibid.

[123] Ibid.

identification mode are referred to as one-to-many because the individual's biometric is compared against multiple templates in the system's database.[124]

There are two types of identification systems: positive identification systems, which are designed to ensure that an individual is enrolled in a database, and negative identification systems, which are designed to ensure an individual's biometric information is not stored in a database.[125] A typical use of positive identification systems is to secure a building or computer room by checking those who seek access against a database of authorized personnel. A negative identification system might be utilized to prevent individuals from registering for federal or state benefit programs multiple times under multiple identities.

2. Biometric Technologies

The evolution of biometric system technology in recent years has moved the technology from rudimentary fingerprint and photograph biometric trait authentication to an expanded list of traits which can be used for identification. Commercial companies and academic researchers have either developed or are researching biometric systems that utilize iris, face, fingerprint, palm print, brain wave, ear shape, hand geometry, knee, vein pattern, voice, gait, DNA and odor traits, among others.[126] Research is being conducted to find methods to use quick X-ray snapshots of a person's internal body parts, such as the knee, which would be more difficult for a criminal to spoof than an artificial fingerprint.[127]

Each biometric system has unique characteristics, capabilities, issues and applications. Of the more than a dozen biometric technologies, only a handful have been

---

[124] United States General Accounting Office (GAO), *Technology Assessment: Using Biometrics for Border Security*, Washington D.C.: GAO, November 2002, 43.

[125] Ibid., 44–45.

[126] Anil K. Jain, Patrick Flynn and Arun Abraham Ross, *Handbook of Biometrics*, New York: Springer, 2007, p. 4. and Science Daily News, *New Biometric ID: A Quick X-Ray Snapshot of a Person's Knee*, March 28, 2009, http://www.sciencedaily.com/releases/2009/03/090325150611.htm (accessed May 1, 2009).

[127] Science Daily News, *New Biometric ID: A Quick X-Ray Snapshot of a Person's Knee*, March 28, 2009, http://www.sciencedaily.com/releases/2009/03/090325150611.htm (accessed May 1, 2009).

tested by government agencies and shown to be ready for deployment on a large scale as would be required to support a national biometric identification program. Several government reports have identified four biometric technologies as being most suitable for border and national security purposes.

The Defense Threat Reduction Agency (DTRA) report on Military Critical Technologies identified six leading biometric technologies, of which the top four biometric systems identified as best suited for military and security applications are fingerprint analysis, facial recognition, hand geometry and iris recognition.[128] The Congressional Research Report on Biometric Identifiers and Border Security identified the same four (fingerprint, facial recognition, hand geometry and iris recognition) leading biometric technologies, all of which are in wide use in North America, Europe, Asia and the Middle East.[129]

Likewise, the Government Accountability Office (GAO) singled out these four for border security projects, stating that all are mature technologies and have been demonstrated effective in government pilot programs or operationally in border control operations.[130] However, the GAO report does note that hand geometry may not be distinct enough to rapidly identify an individual from a large population. The remainder of this section will examine the history, basic technical methods and current status of these four leading biometric technologies.

a. Fingerprinting

A fingerprint is the pattern of ridges and valleys on the surface of the fingertip.[131] Fingerprints are the oldest and most widely-used biometric markers and

---

[128] Defense Threat Reduction Agency, *Military Critical Technologies List: Information-Security Technology*, Ft. Belvoir, VA: Department of Defense, October 2003, 60.

[129] Daniel Morgan and William Krouse, *Biometric Identifiers and Border Security: 9/11 Commission Recommendations and Related Issues*, Report Number: RS21916, Washington D.C.: Congressional Research Service (CRS) Report for Congress, 2005, 2–3.

[130] United States General Accounting Office (GAO), *Technology Assessment: Using Biometrics for Border Security*, Washington D.C.: GAO, November 2002, 4–5.

[131] Anil K. Jain, Patrick Flynn and Arun Abraham Ross, *Handbook of Biometrics*, New York: Springer, 2007, 16.

have been used for personal marks or signatures in parts of Asia as early as the third Century B.C.[132] Since the late 1800s, fingerprints have been collected using ink and paper in Western societies.[133] Fingerprints were one of the first biometric attributes to be used by law enforcement and government agencies for identification. In 1903, the New York Bureau of Prisons established a Fingerprint Bureau to link criminals and their arrests.[134] During World War II, the Federal Bureau of Investigation (FBI) established a fingerprint applicant clearance check system to vet millions of military personnel and defense factory workers.[135] Today, the most widely-used and best-known biometric identification system for law enforcement agencies is the FBI's Integrated Automated Fingerprint Identification System (IAFIS) which contains about 57 million fingerprint sets on file.[136]

In the U.S., fingerprints have been used for decades to match individuals and are generally viewed as an acceptable method of identification. A 1990 study of biometrics found that public acceptance of fingerprinting was 96%.[137] Fingerprints are distinctive, but at the very end of an appendage that could be damaged by cleaning agents or physical injury. Estimates are that 1% to 4% of fingerprints will not register in automated biometric applications.[138] Research into 3-dimensional fingerprinting is ongoing at the University of Kentucky which, if successful, will reduce failure to enroll rates and make it easier to obtain accurate, detailed prints.[139]

---

[132] John D. Woodward, Nicholas M. Orlans, and Peter T. Higgins, *Biometrics: Identity Assurance in the Information Age*, Hightstown, New Jersey: McGraw-Hill Professional, 2002, 45.

[133] Ibid.

[134] Ibid., 48.

[135] Ibid.

[136] James Howe, "Defeating the Unknown Terrorist," *Proceedings*, October 2008, Vol. 134, Iss. 10: 38–42, 40.

[137] Dr. James Wayman, *National Biometrics Test Center: Biometrics Publications*, 2000, http://www.engr.sjsu.edu/biometrics/publications_tech.html (accessed May 20, 2009).

[138] John D. Woodward, Nicholas M. Orlans, and Peter T. Higgins, *Biometrics: Identity Assurance in the Information Age*, Hightstown, New Jersey: McGraw-Hill Professional, 2002, 22.

[139] Rachel Kreman, *Touchless 3-D Fingerprinting: A New System Offers Better Speed and Accuracy*. September 30, 2009, http://www.technologyreview.com/computing/23549/page1/ (accessed October 1, 2009).

Fingerprint systems use a comparison of a sample fingerprint to a person's enrolled template in a database to authenticate an identity. Depending on the technology utilized by the vendor, the size of fingerprint templates range from 250 bytes to 1,000 bytes.[140] The accuracy standard for commercial use of fingerprint biometric systems is no more than one error for every 1,000 scans.[141] Government agencies face the challenge of making one-to-many fingerprint comparisons and getting the forensic quality prints needed for that.[142] The collection of multiple fingerprints from a person provides additional information to facilitate large scale identification systems with millions of records.[143]

Searching databases the size of the FBI's IAFIS to match a single set of fingerprints against millions of stored fingerprint templates could be an extremely time consuming process. To reduce the amount of time required to compare trial fingerprints against template fingerprints stored in large databases, a process called binning is often used. The trial fingerprints are compared to a reference template in the large database and categorized according to the fingerprint type.[144] Figure 2 shows three fingerprint bin categories which can be used to compare trial fingerprints against template fingerprints: plain arch (left), loop (middle) and plain whirl (right).[145] By searching for matches within a specific bin the biometric system can quickly eliminate the bulk of non-matches first by looking at fingerprints which are similar.

---

[140] United States General Accounting Office (GAO), *Technology Assessment: Using Biometrics for Border Security*, Washington D.C.: GAO, November 2002, 47.

[141] Ann Keeton, "Fingerprints Give a Hand to Security: Verifying Identities Through Biometrics is Poised to Expand," *Wall Street Journal*, Apr 12, 2007, B4.

[142] Ibid.

[143] Anil K Jain. Patrick Flynn, and Arun Abraham Ross, *Handbook of Biometrics*, New York: Springer, 2007, 16.

[144] United States General Accounting Office (GAO), *Technology Assessment: Using Biometrics for Border Security*, Washington D.C.: GAO, November 2002, 148.

[145] Ibid.

Figure 2. Binning Fingerprint Types (plain arch, loop and whirl)[146]

Advantages to using fingerprint biometric systems include: individuals have multiple fingers to print; systems are easy to use; there is a large amount of existing data to allow background and watch list checks, technology has proven effective in many large systems over years of use; fingerprints are unique to each finger of each individual; and the ridge arrangement remains permanent during one's lifetime.[147] Disadvantages to using fingerprint biometric systems include: privacy concerns; health and societal concerns with touching a sensor used by countless individuals; and an individual's age and occupation may cause some sensors difficulty in capturing a complete and accurate fingerprint image.[148]

b. Hand Geometry

Hand geometry recognition systems are based on a number of dimensional measurements taken from the human hand, including its shape, palm size, and the lengths and widths of the fingers.[149] They are the second most widely-used biometric system, although no recorded uses of hand tracings were used to differentiate people prior to the introduction of hand geometry readers in the 1980s by Recognition Systems, Inc. (RSI)

---

[146] United States General Accounting Office (GAO), *Technology Assessment: Using Biometrics for Border Security*, Washington D.C.: GAO, November 2002, 148.

[147] National Science and Technology Council, "Biometrics Foundation Documents," *Committee on Homeland and National Security,* August 2006. http://www.biometrics.gov/Documents/biofoundationdocs.pdf (accessed September 2, 2009), 5.

[148] Ibid.

[149] A.K. Jain, R. Bolle and S. Pankanti, *Biometrics: Personal Identification in Networked Society*, London: Kluwer Academic Publishers, 1999, 16.

of California.[150] Today, RSI is a division of Ingersoll-Rand Inc. and sells approximately 90% of hand geometry biometric products sold.[151]

Hand geometry systems utilize a camera to capture an image of the hand. The camera captures the top surface of the hand and a side image (using a side mirror), resulting in a total of 90 or more measurements being taken.[152] A mathematical algorithm is used to determine the unique aspects of the hand and converts the 90 measurements into a 9-byte template, which is the smallest template required of any of the current biometric technologies.[153] Current uses of hand geometry biometric systems include: access control and time and attendance, where hand geometry scanners are used to verify the identity of people punching in and out of work each day.[154]

Hand geometry is one of the easiest methods to use. However, while hands are robust, a person's hand geometry can change from a major injury or suffer loss of dexterity or swelling from arthritis. Advantages to using hand geometry include: small template size, easy to capture and patterns are highly stable over the adult lifespan.[155] Hand geometry is not as distinctive as other biometric identifiers since, "One in 100

---

[150] John D. Woodward, Nicholas M., Orlans, and Peter T. Higgins, *Biometrics: Identity Assurance in the Information Age,* Hightstown, New Jersey: McGraw-Hill Professional, 2002, 65.

[151] Ibid.

[152] National Science and Technology Council, "Hand Geometry," *Committee on Homeland and National Security, Subcommittee on Biometrics,* August 6, 2006. http://www.biometrics.gov/Documents/HandGeometry.pdf (accessed September 2, 2009), 3-4.

[153] United States General Accounting Office (GAO), *Technology Assessment: Using Biometrics for Border Security,* Washington D.C.: GAO, November 2002, 47.

[154] John D. Woodward, Nicholas M. Orlans. and Peter T. Higgins, *Biometrics: Identity Assurance in the Information Age,* Hightstown, New Jersey: McGraw-Hill Professional, 2002, 67.

[155] National Science and Technology Council, "Biometrics Foundation Documents," *Committee on Homeland and National Security,* August 2006. http://www.biometrics.gov/Documents/biofoundationdocs.pdf (accessed September 2, 2009), 6.

people have hands similar to your hand."[156] Disadvantages include: system use requires training and hand geometry may not be sufficiently distinctive for identification if there is a need to search large databases.[157]

c. Iris Recognition

In 1987, Ophthalmologists Leonard Florn and Arin Safir were awarded a patent for describing methods and apparatus for iris recognition based on visible iris features.[158] Doctor Florn subsequently approached Dr. John Daugman of Cambridge University to investigate methods for automating identification of the iris. Dr. Daugman developed algorithms, mathematical methods and techniques to encode iris patterns and compare them.[159] In 1994, Dr. Daugman was awarded a patent, which expires in 2011, for his automated iris recognition systems called IrisCodes.[160] All commercial applications currently implement IrisCodes, and Iridian Technologies, Inc. is the sole owner and developer of iris recognition technology, although hardware products are manufactured by a variety of corporations.[161]

The characteristics of the iris are formed during the eighth month of gestation and will not change except through procedures such as cataract surgery, refractive surgery or cornea transplants.[162] Figure 3 shows the iris location in relation to other parts of the human eye. The iris has numerous forms of variability, and where other

---

[156] Ann Keeton, "Fingerprints Give a Hand to Security: Verifying Identities Through Biometrics is Poised to Expand," *Wall Street Journal*, April 12, 2007, B4.

[157] National Science and Technology Council, "Biometrics Foundation Documents," *Committee on Homeland and National Security,* August 2006. http://www.biometrics.gov/Documents/biofoundationdocs.pdf (accessed September 2, 2009), 6.

[158] John D. Woodward, Nicholas M. Orlans, and Peter T Higgins, *Biometrics: Identity Assurance in the Information Age,* Hightstown, New Jersey: McGraw-Hill Professional, 2002, 90.

[159] Ibid., 91.

[160] National Science and Technology Council, "Iris Recognition," *Committee on Homeland and National Security*, August 7, 2006, http://www.biometrics.gov/Documents/IrisRec.pdf (accessed September 12, 2009), 1–2.

[161] United States General Accounting Office (GAO), *Technology Assessment: Using Biometrics for Border Security,* Washington D.C.: GAO, November 2002, 196.

[162] Ibid., 193.

biometrics have only 13 to 60 distinct characteristics, the iris has 266 unique spots that can be used for identification.[163] Iris patterns differ from person to person, and it has been postulated that the probability of two individuals having the same iris pattern is 1 in 7 billion.[164]

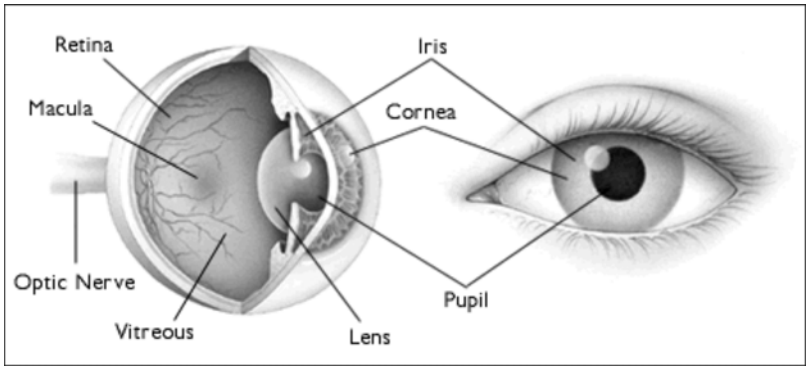

Figure 3. The Iris and Other Parts of the Eye[165]

Iris recognition systems use cameras and infrared illumination to capture an image of the iris's structure. Images are then converted into digital templates which are used to create the IrisCode representations of the iris. The IrisCode is typically a 256-byte representation, although with additional header information it can be as large as 512 bytes.[166] The comparison of a trial IrisCode is conducted by determining the number of mismatched bytes between the trial IrisCode and the IrisCode templates in a biometric system database. The extent to which the IrisCodes of the trial and the templates differ is referred to the Hamming Distance (HD).[167] The key concept to iris recognition is the test of statistical independence. If less than one-third of the bytes in the IrisCodes are different, then the IrisCode fails the test of statistical independence, indicating that the

[163] United States General Accounting Office (GAO), *Technology Assessment: Using Biometrics for Border Security*, Washington D.C.: GAO, November 2002, 196.

[164] Ibid., 193.

[165] Ibid.

[166] John D. Woodward, Nicholas M. Orlans and Peter T. Higgins, *Biometrics: Identity Assurance in the Information Age*, Hightstown, New Jersey: McGraw-Hill Professional, 2002, 92.

[167] National Science and Technology Council, "Iris Recognition," *Committe on Homeland and National Security*, August 7, 2006, http://www.biometrics.gov/Documents/IrisRec.pdf (accessed September 12, 2009), 3.

IrisCodes are from the same iris.[168] Researchers have calculated the odds of two different iris's generating an IrisCode that produces a false match to be 1 in 1.2 million.[169]

Advantages to using iris recognition technology include: there is no physical contact required with sensor equipment, the iris is a protected internal organ which is less prone to injury and the iris characteristics are highly stable over lifetime.[170] Disadvantages include: the characteristics of the iris cannot be verified by a human, there are concerns with scanning of the eye with a light source, the systems require more training and attentiveness than most biometric systems and there is a lack of existing data, which limits the ability to conduct background or watch list checks.[171]

d. Facial Recognition

Facial recognition systems identify individuals through analysis of the unique patterns and contours on an individual's face through thermal imaging, video or still images. The first semi-automated facial recognition system was developed in the 1960s, and required the administrator to locate the position of facial features on photographs before calculating distance and ratios to a common reference point.[172] By 1988, Michael Kirby and Lawrence Sirovich applied a new concept, incorporating a standard linear algebra technique to face recognition analysis called the eigenfaces technique; the result is somewhat of a milestone, as it showed that fewer than 100 values

---

[168] National Science and Technology Council, "Iris Recognition," *Committe on Homeland and National Security*, August 7, 2006, http://www.biometrics.gov/Documents/IrisRec.pdf (accessed September 12, 2009), 3.

[169] John D. Woodward, Nicholas M. Orlans and Peter T. Higgins, *Biometrics: Identity Assurance in the Information Age*, Hightstown, New Jersey: McGraw-Hill Professional, 2002, 93.

[170] National Science and Technology Council, "Biometrics Foundation Documents," *Committee on Homeland and National Security*, August 2006. http://www.biometrics.gov/Documents/biofoundationdocs.pdf (accessed September 2, 2009), 5.

[171] Ibid., 6.

[172] National Science and Technology Council, "Facial Recognition," *Committee on Homeland and National Security*, August 7, 2006, http://www.biometrics.gov/Documents/FaceRec.pdf (accessed September 11, 2009), 1.

were required to accurately code a facial image.[173] In 1991, Matthew Turk and Alex Pentland utilized the eigenfaces technique to establish that residual error could be used to detect faces in images, a discovery that enabled reliable real-time automated face-recognition systems.[174] Today, facial recognition systems are used to allow access to military buildings, for surveillance and monitoring of people in crowds and stadiums, to combat passport fraud and identity fraud, and to support law enforcement.

The two predominant approaches to face recognition include geometric (feature based) and photometric (appearance based).[175] Geometric-based systems use areas, distances, and angles between facial feature points as descriptors for facial recognition.[176] Appearance-based methods consider the global properties of a face image intensity pattern where face recognition algorithms compute basis vectors to represent face data.[177] Depending on the specific technology, the template size of facial recognition samples ranges from 84 bytes to 1300 bytes.[178]

Advantages to using facial recognition systems include: there is no contact with the sensor required, the camera sensors are readily available, large amounts of data exist to facilitate background and watch list checks and the systems are easy for humans to verify results.[179] Disadvantages to using facial recognition include: the face can be obstructed by hair, glasses or a hat; the systems are sensitive to changes in lighting; faces change over time; and there is propensity for users to provide poor quality video or

---

[173] National Science and Technology Council, "Facial Recognition," *Committee on Homeland and National Security,* August 7, 2006, http://www.biometrics.gov/Documents/FaceRec.pdf (accessed September 11, 2009), 1.

[174] Ibid.

[175] Anil K. Jain, Patrick Flynn and Arun Abraham Ross, *Handbook of Biometrics,* New York: Springer, 2007, 44.

[176] Ibid.

[177] Ibid., 45.

[178] United States General Accounting Office (GAO), *Technology Assessment: Using Biometrics for Border Security,* Washington D.C.: GAO, November 2002, 46.

[179] National Science and Technology Council, "Biometrics Foundation Documents," *Committee on Homeland and National Security,* August 2006.
http://www.biometrics.gov/Documents/biofoundationdocs.pdf (accessed September 2, 2009), 6.

pictures and expect accurate results from the recognition systems. [180] Also, facial recognition systems have one of the higher error rates, and it is debatable as to the utility and effectiveness to identify individuals, especially within large crowds such as at a stadium event. An individual's loss of weight, weight gain, plastic surgery or other changes in physical appearance could affect the effectiveness of facial recognition systems.

3. Comparison of Biometric Technologies

Specific biometric technologies may be more appropriate for different applications and the different biometric systems should be assessed based on the requirements. For government organizations, selecting a specific biometric technology involves following the acquisition guidelines outlined in the Federal Acquisition Regulation, meeting developmental and operational testing requirements and staying within federal budget constraints. As for commercial applications, the evolution of biometric systems now provides consumers with numerous options to improve security and resolve identity matching. This section will examine the performance characteristics that are used to assess the accuracy of biometric systems and the technology trade-offs, which both government and commercial organizations must weigh when evaluating whether biometric systems are appropriate for an organization's requirements.

a. Performance Characteristics

The accuracy of a biometric system describes how well a system will perform, and is a key factor in public acceptance of biometric technology use by government organizations. Biometrics is a science, but biometric systems have false positives and false negatives: they are not 100 percent accurate.[181] How can the performances of different biometric systems be compared? There are dozens of

[180] National Science and Technology Council, "Biometrics Foundation Documents," *Committee on Homeland and National Security,* August 2006. http://www.biometrics.gov/Documents/biofoundationdocs.pdf (accessed September 2, 2009), 6.

[181] Ed Sperling, *Forbes: Future of Digital IDs,* May 11, 2009. http://www.forbes.com/2009/05/11/biometrics-security-enterprise-technology-cio-network-biometrics.html (accessed May 13, 2009).

performance statistics that could be used to measure the performance of a biometric system, but four of the most commonly used are failure to enroll, false rejection, false acceptance and the Crossover Error Rate (CER) or Equal Error Rate (EER).[182]

Failure to enroll (FTE) occurs when a biometric trial, submitted during the enrollment process, does not have enough identification points to identify the individual. The FTE problem is often the result of the sensor not capturing the information correctly, the captured sensor data being not of sufficient quality to develop a template or individuals not being properly trained to provide their biometrics.[183] A low FTE is desirable. If a biometric system is tested and found to have a 2 percent FTE, it does not necessarily mean that 2 percent of the time each enrolled user will experience a problem; it is likely that 2 percent of the enrolled population will experience problems 100 percent of the time.

False Rejection Rate (FRR) is the rate at which an authorized user is incorrectly denied acceptance; the FRR is also referred to as the Type I error and the False Non-match Rate.[184] An example of a false rejection is if William presents himself to the biometric system as William and the biometric system incorrectly rejects the claim. FRR errors are represented as the percentage of times the biometric system produces a false rejection. If 1 in 10,000 authentication attempts results in the rejection of a legitimate user, then the FRR will equal 0.01 percent.

The False Acceptance Rate (FAR) is the rate at which unauthorized users are incorrectly accepted as valid; the FAR is also referred to as the Type II error and the False Match Rate (FMR).[185] An example of false acceptance is if Michael claims to be William and the biometric system incorrectly verifies the claim. FAR errors are

---

[182] Harold T. Tipton, and Micki Krause, *Information Security Management Handbook, Sixth Edition*, Boca Raton: CRC Press, 2007, 1303.

[183] National Science and Technology Council, "Biometrics Foundation Documents," *Committee on Homeland and National Security,* August 2006. http://www.biometrics.gov/Documents/biofoundationdocs.pdf (accessed September 2, 2009), 38.

[184] John D. Woodward, Nicholas M. Orlans, and Peter T. Higgins, *Biometrics: Identity Assurance in the Information Age,* Hightstown, New Jersey: McGraw-Hill Professional, 2002, 35.

[185] Ibid.

represented as the percentage of times a biometric system produces a false accept. If 1 in 1,000 authentication attempts results in the acceptance of an illegitimate user, then the FAR is equal to 0.1 percent.

In biometric systems, there is a trade-off between the FRR and the FAR, as the FAR increases the FRR decreases, and vice versa. All biometric systems allow the administrator to adjust the sensitivity thresholds of the FAR and FRR to meet the organizations requirements. An example of the considerations in a national security setting is that it is more important to have a 1 percent rejection rate of individuals (FRR) who should be accepted versus a 1 percent acceptance rate (FAR) of individuals who should not be accepted and who could be potential terrorists. It might be an inconvenience for someone, who should have access, to be stopped by a security guard or a border agent, but allowing someone entry who should not have access could result in criminal acts or a potential terrorist attack.

The Crossover Error Rate (CER) or Equal Error Rate (EER) is a statistic used to characterize biometric system performance in terms of both the FRR and FAR.[186] CER is a good indicator of the overall accuracy of a biometric system and facilitates the analysis and comparison of biometric products from different companies. It represents the point at which the FRR equals the FAR on a receiver operating characteristic curve. The smaller the CER, the more accurate the system. As an example of the significance of the CER, a biometric device with a crossover error rate of 1 percent is better than a device with 2 percent. The CER rate provides an understanding of a biometric device's overall accuracy for product comparison, but individual environments have specific security requirements, which dictate how many false rejection or false acceptance errors are acceptable.[187]

---

[186] John D. Woodward, Nicholas M. Orlans, and Peter T. Higgins, *Biometrics: Identity Assurance in the Information Age,* Hightstown, New Jersey: McGraw-Hill Professional, 2002, 35.

[187] Shon Harris, *CISSP All-in-One Exam Guide,* New York : McGraw-Hill Publishing, 2007, 180.

b. Technology Trade-offs

Once an understanding of the technical and performance characteristics is obtained, the next step in determining which biometric technology is best suited for a particular environment and purpose is to conduct a trade-off analysis of biometric system characteristics. Key factors, important to both federal agencies and commercial companies, include the performance characteristics, FTE, technology costs, ease of use, accuracy, user acceptance, required security level, error incidence and long term stability.

What characteristics are most important? If the technology is being used to secure a nuclear facility or classified military facility, then low error rates (especially FAR) and performance characteristics may be more important than other factors. Most iris recognition systems have false acceptance rates under 1 percent.[188] Low error rates make iris recognition systems ideal for protecting nuclear facilities and classified military facilities. If a large commercial construction company is looking for a sturdy system to verify identity for employee onsite attendance, then a hand geometry system may best meet the requirements. The most important factors in determining whether a biometric system is appropriate for an identified need will vary from organization to organization.

Table 2 shows a sample comparison chart of biometric technologies against quantifiable measures, including: user acceptance, technology costs, factors affecting performance, performance characteristics, variability in the ability to identify individuals over time as they age, time to enroll and the time it takes for a system to process each user.[189] Table 2 illustrates a basic comparison of the costs and benefits of fingerprint, iris, facial and hand geometry, although a more comprehensive analysis of factors would be required by most consumers or government agencies before investing in a specific vendor's biometric system. Large government agencies and commercial companies may require extensive operational testing of several different biometric system products prior to procuring large numbers of biometric systems.

---

[188] Defense Threat Reduction Agency, *Military Critical Technologies List: Information-Security Technology,* Ft. Belvoir, VA: Department of Defense, October 2003, 63.

[189] Paul Reid, *Biometrics for Network Security* , Upper Saddle River, New Jersey: Prentice Hall, 2004, 70–71.

Characteristic	Fingerprint	Iris	Facial	Hand
Cost	Low	High	Moderate	Moderate
Enrollment time estimate	3 minutes, 30 seconds	2 minutes, 15 seconds	3 minutes	1 minute
Transaction time estimate	5 to 19 seconds	12 seconds	10 seconds	6 to 10 seconds
False Rejection Rate (FRR)	0.2% - 36%	1.9% - 6%	3.3% - 70%	0% - 5%
False Acceptance Rate (FAR)	0% - 8%	Less than 1%	0.3% - 5%	0% - 2.1%
User acceptance issues	Hygiene concerns, associated with law enforcement	User resistance	Privacy concerns	Hygiene concerns
Factors affecting performance	Dirty, dry or worn fingertips	Glare or reflections	Lighting, orientation of face, sunglasses	Hand injuries, arthritis, swelling
Variability with ages	Stable	Stable	Affected by aging	Stable

Table 2. Comparison of Biometric Systems (From Homeland Security Biometrics)[190]

B. BIOMETRIC TECHNOLOGY USES

This section will examine federal guidance on biometrics and how biometric technologies are used commercially as a replacement to identification cards and within the federal government as a law enforcement and counterterrorism tool.

1. Federal Government

There are four government communities collecting and using biometric data: homeland security, military, intelligence and law enforcement. Who within the federal government has the responsibility for establishing biometric system standards for all federal agencies? The National Institute for Standards and Technology (NIST) has a close partnership with U.S. government agencies and U.S. industry to help establish formal national and international biometric standards development bodies to accelerate

[190] GlobalSecurity.org., *Homeland Security: Biometrics*, June 2009. http://www.globalsecurity.org/security/systems/biometrics.htm (accessed June 1, 2009).

the development of biometric standards.[191] But, with the national security implications and the enormous federal expenditures on biometric technology, the federal government required a more coordinated approach to ensure interoperability of federally funded biometric systems.

On June 8, 2008, President George Bush signed National Security Presidential Directive–59 (NSPD-59)/Homeland Security Presidential Directive–24 (HSPD-24) entitled Biometrics for Identification and Screening to Enhance National Security.[192] NSPD-59/HSPD-24:

> . . . establishes the framework to ensure federal departments and agencies use mutually-compatible methods and procedures for collection, storage, use, analysis, and sharing of biometric and biographic information while respecting information privacy and other legal rights under United States law.[193]

The Director of the Office of Science and Technology, through the National Science and Technology Council, has been designated as the lead agency for coordinating biometric standards, research, testing and conformance testing for the federal government.[194] NSPD-59/HSPD-24 forced government agencies to begin a cooperative relationship and address issues as basic as establishing definitions and categories for biometric collection and establishing a collaborative environment amongst federal agencies. The following sections examine the use of biometrics by the federal government for criminal investigation, border security and national defense.

a. Federal Bureau of Investigation

In the mid-1990s, the Federal Bureau of Investigation (FBI) established the Integrated Automated Fingerprint Identification System (IAFIS) to manage the

---

[191] National Institute of Standards and Technology (NIST), *National and International Biometric Standards - Development Bodies and Published Standards*, February 2009, http://www.itl.nist.gov/div893/biometrics/standards.html (accessed April 21, 2009).

[192] George W. Bush, *Biometrics for Identification and Screening to Enhance National Security/NSPD-59/HSPD-24*, Washington D.C., June 5, 2008.

[193] Ibid.

[194] Ibid.

millions of fingerprint sets on file.[195] The IAFIS contains 57 million fingerprints sets on file, each set containing prints from all ten fingers.[196] Despite the large number of fingerprint sets on file, six of seven U.S. citizens have never been fingerprinted and more than half of the fingerprints collected are not from criminals, but from law-abiding citizens who have submitted to background checks for employment purposes.[197] Since 9/11, the number of fingerprint searches has increased exponentially; the FBI now checks the identities of approximately 15,000 visa applicants for the U.S. State Department daily; and the IAFIS set a record in 2008 with 147,000 total identification checks in a single day.[198]

The FBI is expected to spend up to $1 billion in the next ten years to enhance identification systems.[199] In 2008, a contract was awarded to Lockheed Martin to develop the Next Generation Identification System (NGIS) for a multimodal biometrics system that will enable the collection and storage of additional biometric data from criminals and terrorists.[200] The FBI is considering using palm prints, iris prints and facial scanning; palm prints may offer the most important improvement for law enforcement, because approximately 20 percent of latent prints gathered at crime scenes are from the palms of criminals.[201] Objectives of NGIS include establishing interoperability with systems operated by DoD, DHS, the intelligence community and eventually the international community, keeping in mind that the system needs to take into account the privacy of individuals, meet data sharing laws and provide security.[202]

---

[195] James Howe, "Defeating the Unknown Terrorist," *Proceedings*, October 2008, Vol. 134, Iss. 10: 38–42, 40.

[196] Ibid.

[197] Stew Magnuson, "Under Watch: Government Seeking Clear Path for Biometric Data Use," *National Defense*, September 2008, Vol. 93, Iss. 658: 23–35, 28.

[198] MaryAnn Lawlor, "Bureau Beefs Up Biometrics Capabilities," *Signal*, September 2008, Vol. 63, Iss. 1: 67–70, 68–69.

[199] Ibid., 68.

[200] Ibid., 68–69.

[201] Ibid., 70.

[202] Ibid., 70.

The FBI is also collecting biometric data in the global war on terrorism. According to the agency, officials who are using fingerprint biometrics technology in Afghanistan to identify individuals on the battlefield have found that the use of biometrics "does bear fruit."[203] Since 9/11, there have been many successes where biometric technology has been used on the battlefield to identify terrorists with ties to the United States. A man stopped at a checkpoint in Tikrit, Iraq claimed to be a dirt poor farmer, but after a biometric fingerprint check with the FBI's biometric criminal records, it turned out the man had 11 felony charges in the U.S., including assault with a deadly weapon.[204] According to one report, in 2004, an FBI team helicoptered to a remote desert camp on the Iraq–Iran border, home to the Mujahedin-e-Khalq (MEK); the FBI team fingerprinted 3,800 fighters, and determined that more than 40 had previous criminal records in the agency's database.[205]

b. Department of Defense

The Department of Defense (DoD) has been at the forefront in implementing biometrics to secure overseas bases and for forensic purposes in Iraq and Afghanistan. According to Paul McHale, the Director of the DoD Biometrics Task Force (BTF):

> Our enemy today is no longer in uniform; our enemy today is probably wearing civilian clothes and is virtually indistinguishable from the innocent . . . biometric identification is an important way to distinguish friend from foe."[206]

The U.S. Army has been established as the executive agent for the DoD BTF.

---

[203] Ellen Nakishima, *Post 9/11 Dragnet Turns Up Surprises: Biometrics Links Foreign Detainees to Arrests in the U.S.*, July 6, 2008. http://www.biometrics.dod.mil/Newsletter/issues/2008/July/v4issue3/v4issue3_add3.html (accessed May 15, 2009).

[204] Ibid.

[205] Ibid.

[206] United States. Department of the Army, "Biometrics Task Force: DoD ABIS," *BTF Trifold.*

Many of the current biometric capabilities being developed by DoD are to assist U.S. troops with identifying potential terrorists in Iraq and Afghanistan. In 2003 and 2004, U.S. troops lacked the necessary capabilities to identify individuals passing through checkpoints and entering U.S. bases to perform day labor, making personnel vulnerable to terrorist attack. In 2005, the U.S. Army awarded a $20 million contract to Northrop Grumman Corporation to develop a biometric solution to resolve issues relating to the identification of individuals.[207]

The primary biometric identification capability that resulted from the contract is the Automated Biometric Identification System (ABIS).[208] The ABIS is being used in a variety of ways, such as storing of forensic evidence from crime scenes, including fingerprints taken from improvised explosive devices, and sniper attack locations. The ABIS biometric system registers people by their fingerprints, iris patterns and other biological metrics. After the information is collected, the data is relayed back to the U.S. where the data is used by law enforcement and intelligence agencies to identify individuals and search for connections between individuals. Military members register individuals within the community and at check points and base access points using portable biometric scanners. The collection of biometric data has been extensive. According to Colonel Eloy Campos:

> During my tenure in Iraq we collected in excess of 250,000 biometric scans on the local populace … this data led to the issue of resident identification cards … [and] on multiple occasions the resulting biometrics led our forces to insurgents and centers of activity.[209]

---

[207] Christian Lowe, *Biometrics Track Bad Guys*, February 23, 2007. http://www.defensetech.org/archives/003306.html (accessed May 22, 2009).

[208] Department of the Army, *DoD Biometrics Task Force Homepage*, 21 2009, May. http://www.biometrics.dod.mil/ (accessed May 21, 2009).

[209] Colonel Elroy Campos, *Consolidating Our Country's Biometric Resources and the Possible Implications*, Carlise Barracks: U.S. Army War College, 2008, 2.

The ABIS contains around 3 million records and utilizes multimodal biometrics.[210] Multimodal biometrics uses more than one technology to secure an identification match. If there is only a partial set of fingerprints and a photo of poor quality, the data can be used in context with other information, which may result in a positive match. According to Lisa Swan, deputy director for the DoD Biometrics Task Force, "You get a score on the fingerprint that's not high and the face that's not high, but fused together it will provide a potential match."[211] The DoD is working with the FBI to make DoD ABIS and the FBI's Next Generation Identification System (NGIS) interoperable.

Within the DoD, biometrics technology is not just limited to data collection and analysis on the battlefield. Many DoD organizations within the continental U.S. and at overseas bases are using biometrics systems to address base security issues. The U.S. Air Force (USAF) Air Education and Training Command (AETC) implemented biometric identification systems at all base entry points. Gate guards at Air Force bases are using handheld scanners to implement the Defense Biometric Identification System (DBIS). The scanner reads the bar codes on DoD Common Access Cards and can tell instantly whether a person is allowed on the base or not.[212] The biometric and biographical data attributes stored in DBIS include: name, age, height, photograph, fingerprints, address, telephone number, e-mail address, birthplace, nationality, education level and group affiliation. The DBIS database is connected with the Defense Enrollment Eligibility Reporting System (DEERS) that provides data on active-duty members, civilians, retired members and dependents.[213] During periods of higher force protection, additional information can be added to the DBIS locally.[214]

---

[210] Zack Martin, *Biometrics and the Department of Defense*, September 16, 2009. http://www.secureidnews.com/2009/09/16/biometrics-and-the-department-of-defense (accessed September 18, 2009).

[211] Ibid.

[212] Captain John Severens, AETC Officials to Automate Entry Control, May 7, 2009. http://www.af.mil/news/story.asp?id=123148134 (accessed May 20, 2009).

[213] Ibid.

[214] Ibid.

In Southwest Asia, the 379th Expeditionary Security Forces Squadron (ESFS) is using DBIS to process more than 1,600 third-country nationals (TCNs) daily who work on an overseas military base.[215] The TCNs perform a wide range of support functions on many overseas military installations, including: food service, transportation, laundry and construction. The data collection begins when an individual is hired by a unit or organization, and once data is collected, the individual must be cleared through DBIS. The data collected is sent through the DoD Biometrics Fusion Center (BFC), located in West Virginia, which maintains an archive of DBIDS data from military installations worldwide. After that, the data is run against several law enforcement databases, including the FBI's Most Wanted Terrorists list.[216] If the TCN receives approval from the BFC, then the individual will be processed for a TCN badge. The TCN's are required to scan in when entering and existing the installation each day. According to Airman Ramirez, currently deployed with the 379th ESFS, "knowing who is on the installation at all times and having a biometric system that tracks TCN's allows for increased protection of every service member and is an asset on base."[217]

Discussion is ongoing within DoD on what biometrics might be incorporated in the Common Access Card (CAC) in the future. The CAC is issued to military members, civilian employees and contractors, and enables access to military installations, receipt of benefits and access to DoD computer systems. According to Lisa Swan, deputy director for the DoD Biometrics Task Force, "Using biometrics with the CAC is in the future plans…for more secure applications you will see biometrics fairly soon, it's just a matter of what's practical and what you're trying to safeguard."[218] Swan continued, "the CAC will eventually be used with the biometric to access different

[215] Senior Airman Michael Matkin, *Biometric Database Offers Security Stamp of Approval*, August 10, 2009, http://www.af.mil/news/story.asp?id=123162638 (accessed September 10, 2009).

[216] Ibid.

[217] Ibid.

[218] Ibid.

computer records [including health records] . . . our soldiers are more mobile now and this is something that could tie them to their records."[219]

c. Department of Homeland Security

The Department of Homeland Security (DHS) United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program is the U.S. entry-exit program for foreign travelers and provides biometric technology to visa-issuing ports of entry. The goals of the US-VISIT include: enhance the security of U.S. citizens and visitors, facilitate legitimate travel and trade, ensure the integrity of the U.S. immigration system and protect the privacy of visitors.[220] The process begins at a U.S. issuing post where a traveler's biometrics—10 digital fingerprints and a photograph—are collected and checked against watch lists for known criminals and terrorists. Later, when a traveler arrives in the U.S., the same biometrics are collected to verify identity at the port of entry.[221] Currently, US-VISIT entry capabilities are operating at over 300 land, sea and air ports.[222] Exit capabilities are not yet operating but, pilot efforts are underway.

Robert Mocny, US-VISIT Director for DHS, stated "when we did the pilots [for exist procedures] between 2004 and 2007, we determined quickly that the [biometric] technology worked . . . what didn't work was the process . . . you usually don't check out of the U.S., so the exit process is really new to people."[223] In June 2009, DHS conducted an exit-tracking pilot program at Hartsfield International Airport in Atlanta, GA, during which Transportation Security Administration personnel with

---

[219] Zack Martin, *Biometrics and the Department of Defense*, September 16, 2009. http://www.secureidnews.com/2009/09/16/biometrics-and-the-department-of-defense (accessed September 18, 2009).

[220] United States Government Accountability Office (U.S. GAO), *Homeland Security: US-VISIT Program Planning and Execution Improvements Needed*, Report to Congressional Commities, Washington D.C.: U.S. GAO, December 2008, 15.

[221] Department of Homeland Security, *US-VISIT Travelor Information* , May 29, 2009. http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0006.shtm (accessed June 16, 2009).

[222] United States Government Accountability Office (U.S. GAO), *Homeland Security: US-VISIT Program Planning and Execution Improvements Needed*, Report to Congressional Commities, Washington D.C.: U.S. GAO, December 2008, 1.

[223] Jill Aitoro, *DHS Launches Second Test of Biometric Exit Processes*, June 10, 2009. http://www.nextgov.com/nextgov/ng_20090610_9479.php (accessed June 11, 2009).

handheld computers collected fingerprints, passport and visa data.[224] Based on the results of the pilot program, the DHS will determine the best approach for collecting biometric information. By March of 2010, a final rule for exit procedures at all airports and seaports will be issued.[225]

The U.S. Immigration and Customs Enforcement (ICE) agency has received $1.6 billion from Congress to implement the Secure Communities program, which is chartered to identify and remove criminal aliens from the U.S.[226] Secure Communities distributes both the FBI's IAFIS biometrics-based criminal records, and the DHS's biometric-based immigration history about inmates, and streamlines the process under which an arrested individual can be identified as a removable criminal alien. The Secure Communities program is currently available to law enforcement agencies in 50 counties nationwide, and will eventually be made available to all state and local law enforcement agencies throughout the nation.[227]

Both local law enforcement agencies and federal officials believe the program will be very successful in helping to remove criminals and individuals identified on terrorist watch lists. According to Sheriff Amadeo Ortiz, from Bexar County Texas, "This is a win-win situation for the community and law enforcement . . . we are able to identify illegal immigrants who commit crimes . . . and get them in the process for deportation, and it does not require additional funds or manpower for us."[228] Robert Mocny, US-VISIT Director, stated "by enhancing the interoperability of DHS's and the FBI's biometric systems, we are able to give federal, state and local decision makers

---

[224] Jill Aitoro, *DHS Launches Second Test of Biometric Exit Processes*, June 10, 2009. http://www.nextgov.com/nextgov/ng_20090610_9479.php (accessed June 11, 2009).

[225] Ibid.

[226] United States Immigration and Customs Enforcement, *ICE: Secure Communities Program* , May 14, 2009, http://www.ice.gov/pi/news/factsheets/secure_communities.htm (accessed May 21, 2009).

[227] Imperial Valley News - Yuma, AZ, *Program Broadened to Enhance Identification and Removal of Criminal Aliens*, June 16, 2009. http://www.imperialvalleynews.com/index.php?option=com_content&task=view&id=5910&Itemid=1 (accessed June 16, 2009).

[228] Ibid.

information that helps them better protect our communities and our nation."[229] The Secure Communities program has enormous potential. In fiscal year 2008, ICE identified more than 221,000 potentially-removable aliens incarcerated nationwide.[230]

DHS is sponsoring research and development in biometric technology. On September 21, 2009, the Unisys Corporation, working under contract with DHS and the Defense Information Systems Agency, announced the completion of a successful demonstration of sharing iris recognition biometric data across three vendor products.[231] The project demonstrated, for the first time, the ability to integrate different products, thus eliminating the need to limit iris recognition to a single vendor in US-VISIT. DHS, Draper Laboratory and several other organizations are sponsoring a program called Future Attribute Screening Technology (FAST).[232] The FAST project, which is expected to be completed by 2011, will utilize thermal imaging cameras and non-invasive biometric sensors that monitor involuntary physiological reactions, including eye blinks, heart rate, respiration, nervous activity and fidgeting.[233] The technology could be used by CBP officers at border crossings or by Transportation Security Administration personnel to screen personnel prior to boarding aircraft.

2. Commercial

Commercial companies and businesses have been at the forefront in the use of many biometric technologies. Casinos, large amusement parks, banks, schools, and many

---

[229] Imperial Valley News - Yuma, AZ, *Program Broadened to Enhance Identification and Removal of Criminal Aliens,* June 16, 2009. http://www.imperialvalleynews.com/index.php?option=com_content&task=view&id=5910&Itemid=1 (accessed June 16, 2009).

[230] Ibid.

[231] Reuters - Latest News, *Unisys Announces Successful Multi-Vendor Interoperability of Iris Recognition Technology for Homeland Security,* September 21, 2009. http://www.reuters.com/article/pressRelease/idUS73560+21-Sep-2009+BW20090921 (accessed September 24, 2009).

[232] Carolyn Johnson, *Spotting a Terrorist: Next-Generation System for Detecting Suspects in Public Settings Holds Promise, Sparks Privacy Concerns,* September 18, 2009. http://www.boston.com/news/local/massachusetts/articles/2009/09/18/spotting_a_terrorist/ (accessed September 22, 2009).

[233] Ibid.

sports stadiums are incorporating biometric capabilities into their businesses to improve security, conduct crowd surveillance and minimize the possibility of theft or fraud. Banks are using biometric systems for physical security and ATM transactions. Casinos are using biometric facial recognition systems to identify criminals and prohibit problem gamblers from playing casino games. There are numerous books and journals published that explore the commercial applications of biometric systems. This section is limited in scope, but will briefly examine how Walt Disney theme parks and schools are using biometric systems as a replacement to identification cards.

a. Amusement Parks

As an alternative to using photo identification checks, in 1996 Walt Disney theme parks started using biometrics, recording the geometry and shape of visitors' fingers to prevent ticket fraud or resale of tickets. In 2006, all Walt Disney theme parks completed a technology upgrade, replacing the geometry readers with a system that scans fingerprint information. According to Kim Prunty, a Walt Disney World spokesperson, "the new [biometric] system will be easier for guests to use and will reduce wait times."[234] According to Arnold Tang, a theme park consultant, theme parks use biometric technology not only because it is more convenient for guests, but also because the systems are more accurate than photo identification cards.[235] Tang stated about traditional photo identification checks, "There is a lot of subjectivity, and people can look at a photo and identify it differently."[236]

After the 9/11 terrorist attacks, federal government agencies sought out Disney's advice on security and biometrics. According to Jim Wayman, Director of the National Biometric Test Center at San Jose State University, the government may have wanted Disney's expertise because Walt Disney Theme Parks are responsible for the

---

[234] Karen Harmel, *Walt Disney World: The Government's Tomorrowland?* September 1, 2006. http://newsinitiative.org/story/2006/09/01/walt_disney_world_the_governments (accessed September 4, 2009).

[235] Ibid.

[236] Ibid.

U.S.'s largest commercial application of biometrics.[237] Wayman stated, "The government was very aware of what Disney was doing, everybody's interested in a successful project."[238] Biometric industry representatives indicate that Disney has expressed interest in other biometric technologies, including automated facial recognition, which could be used to identify criminals or terrorists in large crowds.

b. Schools

San Diego State University (SDSU) was one of the early pioneers to use biometric technology instead of student identification cards to secure buildings and limit unauthorized access to facilities. In 1998, SDSU purchased 12 hand geometry readers from Ingersoll Rand Security Technology, and installed them at six entrances of the SDSU's Aztec Recreation Center and at the school's Aquaplex.[239] To access the facilities, the individual must be a registered student or an employee of SDSU, present their hand to be read by the biometric system and type in a personal identification number (PIN). If the PIN matches and the hand geometry reading is verified, the individual is granted access to the facility. Prior to the installation of the biometric system, students could easily transfer identification cards to another person for admission to the center. Vicki Greene, member services coordinator for SDSU, stated, "Identification card switching is very big in the fitness club industry, [with biometrics] no longer do members need to bring an identification card, this also means we don't need to have an employee out front checking cards."[240]

The number of colleges installing biometric systems on campuses has increased in recent years. In 2009, several University of California campuses and Baylor University installed hand geometry biometric systems at facility entrances to increase

---

[237] Karen Harmel, *Walt Disney World: The Government's Tomorrowland?* September 1, 2006. http://newsinitiative.org/story/2006/09/01/walt_disney_world_the_governments (accessed September 4, 2009).

[238] Ibid.

[239] CR80News, *Hand Geometry Verifying Sand Diego State Students Since 1998*, May 28, 2009. http://www.cr80news.com/2009/05/28/hand-readers-verifying-san-diego-state-students-since-1998 (accessed September 4, 2009).

[240] Ibid.

security and improve efficiency. According to John Atkinson, identification system administrator at Baylor University, "they provide security . . . it is also convenient to use."[241]

During school hours, many K-12 schools require adults requesting access to the school grounds to present a picture identification card to administrative personnel and sign in. As a replacement to identification card checks, a few schools are now incorporating biometric systems, which not only track who is in the school, but where they are in the school. In August 2009, the Boyd School, a Montessori school with seven locations in Northern Virginia, installed a biometric system designed to confirm the identity of adults entering the school, as well as track students throughout the school day.[242] The biometric system, called BioSafe, was designed specifically for the school and utilizes new near-infrared hand-vein scanning hardware from Identica.[243]

The BioSafe system completely digitizes the act of dropping off and picking up children. Parents will present their hand to a scanner and enter a PIN into a touch-screen computer. The parent enters which children they are dropping off as well as typing in any special instructions for the teachers. Once the parent is approved for access, the parent and child are then authorized entry into the building. The teacher receives notification of the student's arrival and electronically checks them in once they arrive in the classroom. The teacher can subsequently check them in and out of the classroom throughout the day, allowing administrators knowledge of the students' locations at all times. The school is also integrating cameras into the BioSafe biometric system at one of the school campuses. According to Faith Smith, logistics coordinator,

[241] Jenna Thompson, *Hand Scanners Bring Convenience to SLC*, September 9, 2009. http://www.baylor.edu/lariat/news.php?action=story&story=60983 (accessed September 10, 2009).

[242] Leischen Stelter, *Biometrics to Ensure Parents Leave with the Right KID's*, August 11, 2009. http://www.securitydirectornews.com/?p=article&id=sd20090896kXm7 (accessed September 12, 2009).

[243] Ibid.

"Once a parent has checked in their child, during any type of emergency we know exactly who's in the building and whom to evacuate, the system prints out the child's picture and information and teachers take that out with them and make sure all kids are accounted for."[244]

[244] Leischen Stelter, *Biometrics to Ensure Parents Leave with the Right KID's,* August 11, 2009. http://www.securitydirectornews.com/?p=article&id=sd20090896kXm7 (accessed September 12, 2009).

THIS PAGE INTENTIONALLY LEFT BLANK

IV. COURSES OF ACTION

A. ALTERNATIVES

Analysis of alternatives is an analytical comparison of options, which identifies potentially viable solutions to problems. To address the issues with driver's licenses and identification cards identified by the 9/11 Commission several courses of action are possible. This section will analyze the Enhanced Driver's License (EDL) and options based on information covered in previous chapters of this thesis, including: implementing the REAL ID Act of 2005 (RIA), repealing the RIA, replacing the RIA with the PASS ID Act, and establishing a national identification card standard that incorporates biometric technologies.

1. Enhanced Driver's License

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) mandated that the Department of Homeland Security (DHS) and the Department of State (DoS) develop and implement a plan to require U.S. citizens and foreign nationals to present a passport or other appropriate identity and citizenship documentation when entering the U.S. from within the Western Hemisphere by land or by sea.[245] The Western Hemisphere Travel Initiative (WHTI) is the joint DHS and DoS plan that implements the requirements outlined in the IRTPA.

In order to comply with the requirements of the WHTI, several states have begun to issue EDLs, and the DoS is now issuing passport cards.[246] The EDLs and passport cards are approved alternative travel documents to a U.S. passport book for re-entry into the U.S. at land and sea borders when traveling from Canada, Mexico and the

[245] Department of Homeland Security, *Publication of Western Hemisphere Travel Initiative*, March 27, 2008, http://www.dhs.gov/xnews/releases/pr_1206635771151.shtm (accessed April 10, 2009).

[246] Section 7209 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458, 118 Stat. 3638, Dec 17, 2004) is referred to as the Western Hemisphere Travel Initiative (WHTI).

Caribbean.[247] The EDL is a dual-purpose card, which is a driver's license that can also be used for re-entry at border crossings.[248] DHS must approve the application, verification and implementation process of a state's EDL program before a state is authorized to begin issuing EDLs. The issuance of an EDL involves a more rigorous application process than is required to obtain a standard driver's license. To apply, applicants must present documentation showing: a valid Social Security number, U.S. citizenship (from original source documents, such as birth certificate), identity verification (a photo identification card), and residency. In addition, they must have a personal interview with a licensing service representative to verify the information on the application.[249]

a. Card Characteristics

EDLs are required to meet the same card characteristic requirements as REAL IDs. In addition, to assist with human identity verification, EDLs (like passport books and passport cards) are required to contain a passive radio frequency identification (RFID) tag.[250] RFID tags contain an integrated circuit that is capable of storing a unique serial number or other information, and an antenna.[251] The DHS standard for the EDL, passport books and passport cards requires that the passive RFID tags store and transmit only a reference number and not contain any personal identification information. The RFID tags used in EDLs are low in cost, operate at 13.56 MHz, activate only when initiated by an RFID reader and have a limited read range of up to 30 feet.[252]

---

[247] Department of Homeland Security, *Enhanced Driver License: What are they?* June 2009. http://www.dhs.gov/xtrvlsec/crossingborders/gc_1197575704846.shtm (accessed July 23, 2009).

[248] Ibid.

[249] Service Representative, Michigan Department of State, data provided to author, *Questions on Enhanced Driver's License* (September 28, 2009).

[250] Section 7209 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Pub. L. 108-458, 118 Stat. 3638, Dec 17, 2004) is referred to as the Western Hemisphere Travel Initiative (WHTI).

[251] RFID Journal, *The Basics of RFID Technology*, August 5, 2009. http://www.rfidjournal.com/article/print/1337 (accessed August 14, 2009).

[252] United States Government Acountability Office, *Information Security: Radio Frequency Identification Technology in the Federal Government*, Washington D.C.: U.S. GAO, May 2005, p. 9; and Smartrac Group. *e-Passport RFID's.* July 14, 2009, http://www.smartrac-group.com/en/personalausweise.php (accessed August 15, 2009).

The use of RFID technology has raised concerns by privacy advocates who are worried that the technology is vulnerable to unauthorized tracking. To address privacy concerns and limit the potential tracking range, all states issue EDLs with protective sleeves that are designed to shield the EDL RFID tag from being read by an unauthorized RFID reader.[253] Researchers at the University of Washington and RSA Laboratories, however, found while testing the data security of EDLs that the card is readable under certain circumstances in a crumpled sleeve, though not in a well-maintained sleeve. Further, the test demonstrated that even in the protective sleeve in pristine condition, a reader could skim data from the RFID tag at half a yard.[254]

EDLs are intended to quickly provide Customs and Border Patrol (CBP) officers the information required to process individuals crossing U.S. borders. As individuals holding EDLs, passport books and passport cards approach a border patrol agent booth, they are instructed to remove the RFID-enabled travel documents from their protective sleeves and hold them outside their vehicle windows.[255] The passive RFID tag will receive the frequency coming from a border booth RFID receiver and then begin broadcasting the tag's unique identification number. The receiver will acquire the identification number and send the information to a secure database system for lookup.[256] If a match occurs, the Customs and Border Patrol (CBP) Officer can pull up biographic and biometric data associated with the number and initiate verification of the identity of the approaching individual.[257] In the event that the RFID tag does not register with

---

[253] Alice Lipowicx, *DHS Expands RFID use at Borders Today*, June 1, 2009. http://www.fcw.com/Articles/2009/06/01/DHS-expands-RFID-use-at-borders-today.aspx (accessed August 15, 2009).

[254] Todd Lewan, *Special Alloy Sleeves Urged to Block Hackers?* , July 11, 2009, http://www.sfgate,com/cgi-bin/article.cgi?f=/n/a/2009/07/11/financial/f113716D08,DTL (accessed August 19, 2009).

[255] United States Customs and Border Patrol, *Learn to Use Your RFID Enabled Documents,* May 11, 2009. http://www.cbp.gov/xp/cgov/newsroom/multimedia/video/travel_videos/rfid_enabled/ (accessed September 11, 2009).

[256] United States Department of State, *U.S. Passport Card Frequently Asked Questions,* May 2009. http://travel.state.gov/passport/ppt_card/ppt_card_3921.html (accessed August 15, 2009).

[257] Ibid.

information stored in the database, the CBP can scan and read the Machine Readable Zone (MRZ) or barcode that is required on all passport books, passport cards and EDLs.[258]

b. Current Status

Currently, only U.S. citizens living in Michigan, New York, Vermont and Washington State have the option to obtain an EDL. The EDL costs $15 to $30 more than standard driver's licenses, but provides a more convenient and less expensive option than a passport book, which costs $100 and can take months to obtain due to a backlog of requests at the DoS.[259] As of May 12, 2009, thousands of EDLs had been issued, with New York having issued 73,000, Washington over 56,000, Michigan 1,600 and Vermont 2,400.[260] To facilitate trade and tourism between the U.S. and Canada, four Canadian provinces, including British Columbia, Manitoba, Ontario and Quebec, have worked with DHS to develop and produce EDLs.[261] As of May 2009, 12,000 EDLs had been issued by the four Canadian Provinces.[262]

c. Assessment

States issuing EDLs require applicants to provide original source documents for verification of U.S. citizenship, but the data in the EDL is only as good as the source documents. The source document verification process may prohibit some illegal immigrants and criminals from acquiring EDLs, although source documents, such

---

[258] United States Department of State, *U.S. Passport Card Frequently Asked Questions,* May 2009. http://travel.state.gov/passport/ppt_card/ppt_card_3921.html (accessed August 15, 2009).

[259] State of Michigan Department of State, *Enhanced Driver's Licenses Arrive,* April 21, 2009. http://www.michigan.gov/sos/0,1607,7-127--213322--,00.html (accessed August 15, 2009)

[260] Department of Homeland Security, "Fact Sheet on Enhanced Driver's Licenses," *U.S. Customs and Border Protection,* May 29, 2009, http://www.cbp.gov/linkhandler/cgov/travel/vacation/enhanced_dl_fs.ctt/enhanced_dl_fs.doc (accessed August 19, 2009).

[261] Alice Lipowicx, *DHS Expands RFID use at Borders Today,* June 1, 2009. http://www.fcw.com/Articles/2009/06/01/DHS-expands-RFID-use-at-borders-today.aspx (accessed August 15, 2009).

[262] Department of Homeland Security, "Fact Sheet on Enhanced Driver's Licenses," *U.S. Customs and Border Protection,* May 29, 2009, http://www.cbp.gov/linkhandler/cgov/travel/vacation/enhanced_dl_fs.ctt/enhanced_dl_fs.doc (accessed August 19, 2009).

as a birth certificate, may be easier to counterfeit than many other identity documents. A skilled criminal or terrorist may be able to supply counterfeit source documents and obtain an EDL. Requiring fingerprints would provide an additional level of security to the background checks and establish whether the applicant has a criminal status, which could be identified by checking the FBI's IAFIS, the DHS's US-VISIT, and other federal records databases.

The cost to produce, implement and manage EDL programs is relatively low. The EDL is valid for 8 years, making the cost to individuals, based on a maximum additional cost of $30 per issuance, less than $3.75 per year. As an example of the implementation costs, which are in addition to the card costs, Vermont was able to fully implement an EDL program at a cost of $1 million.[263] However, Vermont is only able to issue EDLs at one DMV location and the state has a very small population, around 621,000 people.[264] Implementation of an EDL-type identification program on a national level, to cover the 245 million driver's license and identification card holders, is estimated to cost at least several hundreds of millions of dollars.[265]

DHS has addressed privacy concerns by requiring states to use passive RFID tags, that contain no personal information, and advising states to issue EDLs with protective sleeves to limit the RFID tag's tracking range. Even if the RFID tag information is extracted by an unauthorized RFID reader, the only information that could be obtained is the RFID tag's unique identification number.

RFID tags are a viable alternative to barcode technology, which is currently used by most states to store information on driver's licenses and identification cards. In the U.S., there are currently millions of RFID-enabled identification documents

---

[263] Zack Martin, *New Driver License Legislation Proposed*, September 19, 2009. http://www.secureidnews.com/2009/09/19/new-driver-license-legislation-proposed (accessed September 24, 2009).

[264] United States Census Bureau, *Vermont 2008 Population Estimate*, September 4, 2009. http://quickfacts.census.gov/qfd/states/50000.html (accessed September 14, 2009).

[265] Nikki Swartz, "REAL ID to Cost $11 Billion Plus," *Information Management Journal*, Jan/Feb 2007; 41, 1: 12.

in use. In 2008, the DoS issued over 15 million RFID passport books.[266] As of May 2009, over 1 million RFID passport cards have been issued.[267] By 2017, all of the 70 million U.S. passports in circulation will have been replaced with an RFID-enabled identification document.[268] As more Americans obtain RFID-enabled passport identification documents, and become accustomed to using RFID technology, public acceptance of the technology should increase and privacy concerns decrease.

EDLs are considered more secure than standard driver's licenses and identification cards, but still have vulnerabilities, such as reliance on a photograph and biographical information to establish identity, which could be exploited by criminals and terrorists. Photographs can be altered easily, and also depend on humans to make matches. During the 8 years that an EDL is valid, if an individual changes their appearance, matching the EDL photograph to the individual becomes a challenge. Adding more rigorous verification checks, fingerprints or other biometrics would further secure EDLs.

2. REAL ID ACT

Chapter II included a comprehensive analysis of the costs, benefits, privacy concerns and proponent and opponent arguments for and against the RIA. The RIA fulfills a key 9/11 Commission recommendation requiring states to meet minimum security standards for issuance, and outlines the standard required for a driver's license to be accepted for federal purposes. Factors that limit the effectiveness of the RIA in fully addressing the 9/11 Commission recommendations are that the RIA is voluntary, and does not limit states on the types of identification cards that can be issued or to whom they may issue them. Similar to EDLs, reliance on a photograph as the primary biometric is a major vulnerability since the use of photographs alone may not be sufficient to secure

---

[266] United States Department of State, *Passports*, August 17, 2009. http://travel.state.gov/passport/passport_1738.html (accessed August 17, 2009).

[267] United States Department of State, *U.S. Passport Card Frequently Asked Questions*, May 2009. http://travel.state.gov/passport/ppt_card/ppt_card_3921.html (accessed August 15, 2009).

[268] Kirit Radia, *Passports Go High-Tech*, August 14, 2006. http://i.abcnews.com/Politics/Story?id=2313170&page=1 (accessed September 28, 2009).

driver's licenses and identification cards. Adding a requirement to the RIA to incorporate additional biometric indicators in driver's licenses and identification cards would improve on a well-intended legislative effort to address the 9/11 Commission recommendations.

In 2008, DHS granted $17 million to Mississippi, Wisconsin and Florida to partner in a program that would help other states meet the information sharing requirements of the RIA, including integration of DMV databases.[269] Privacy advocates are concerned that the RIA requirement to link state DMV databases creates a tool the federal government could use to conduct surveillance on legal residents, and that the large databases would be vulnerable to theft and hackers. However, the requirement to integrate state DMV databases provides a mechanism to assist states with identifying criminals and terrorists, like the 9/11 terrorists, who attempted to acquire multiple driver's licenses from multiple states. DHS should continue to fund this effort as it is critical to the success of the RIA or any alternative identification system reform efforts.

3. REPEAL REAL ID ACT

Repealing the RIA would not address any of the 9/11 Commission recommendations. Fifteen states have passed legislation prohibiting implementation of RIA requirements, but the current political environment and makeup of the Senate and Congress does not make repealing the RIA and replacing it with nothing a likely course of action. According to Janice Kephart, a former member of the 9/11 Commission and director of national security policy at the Center for Immigration Studies, "As much as the Senate has not liked REAL ID I don't think any senator wants to be pinned with rolling back a 9/11 Commission recommendation."[270] Since several states will not meet the RIA material compliance requirements prior to the January 2010 deadline, it is

[269] Janice Kephart, *Secretary Chertoff's Stocking Stuffer: States Get Infusion of Secure ID Monies*, December 19, 2008, http://cis.org/kephart/chertoffsstockingstuffer (accessed September 21, 2009).

[270] Zack Martin, *New Driver License Legislation Proposed*, September 19, 2009. http://www.secureidnews.com/2009/09/19/new-driver-license-legislation-proposed (accessed September 24, 2009).

probable that RIA will be amended or replaced with alternative legislation; otherwise, residents of these states may not be able to board aircraft or may be forced to undergo additional airport security measures.

4. PASS ID ACT

Proponents argue that the PASS ID Act is a more flexible approach to securing driver's licenses and identification cards. Opponents argue that it repeals substantive components of the REAL ID Act, freezing standards as they are today to save costs instead of strengthening standards to improve national security. DHS has not provided a detailed cost breakdown of the PASS ID Act, but initial estimates indicate the bill would cost the states less than the RIA. The PASS ID Act requires the same driver's license and identification card characteristics as the RIA. A photograph is the primary biometric identifier, three levels of integrated security features are required and a 2-D barcode will contain the same information as in a REAL ID card. The cost savings features of the PASS ID Act eliminate the requirement for information sharing among state DMV databases, weaken airport security and allow states options to make identity verification determinations. The PASS ID Act would eliminate grants to states to facilitate information sharing and replace the program with a demonstration project that may not produce any useful system.[271] Since the RIA became law, the PASS ID Act is the only driver's license and identification card reform bill to make it out of a Senate or Congressional Committee, but it is not known whether PASS ID has enough public and political support to pass a full Senate and House of Representatives vote.

5. NATIONAL BIOMETRIC-BASED ID SYSTEM

The following subsections examine the use of multimodal biometrics with a national identification card and the suitability of alternative biometrics technologies.

[271] Spencer Hsu, *Administration Plans to Scale Back REAL ID Law*, June 14, 2009. http://www.washingtonpost.com/wp-dyn/content/article/2009/06/13/AR2009061302036.html (accessed September 21, 2009).

a. Multimodal Biometric Identification

A multimodal biometric system consolidates information from multiple biometric sources, providing better performance than identification systems like state driver's license and identification cards systems that utilize a single biometric modality, i.e., the face. As highlighted in Chapter III, biometric systems based on a single modality, such as face, finger or iris, are not 100% accurate because of sensor issues, lack of distinctiveness of the biometric trait, unacceptable error rates and spoof attacks.[272] Multimodal biometric systems can overcome many of these problems by combining multiple attributes or pieces of evidence about an individual to create a more comprehensive picture.[273] Multimodalities also can drastically reduce the size of the non-enrollable population, because of the unlikelihood that the same individual will have problems with all biometric indicators.[274]

The U.S. has demonstrated the willingness, knowledge and capability to implement large-scale multimodal biometric identification systems. The DoD ABIS contains 3 million records (fingerprints, iris scans and biographical metrics) from residents, criminals and terrorists from Iraq and Afghanistan. The DHS US-VISIT program requires visitors to the U.S. to provide 10 fingerprints and a photograph, and contains millions of biometric records. The FBI is implementing the Next Generation Identification program, a multimodal biometric system that will contain the 57 million fingerprints contained in IAFIS, along with photographs and other biometric indicators. DoD, DHS and the FBI are working towards making the databases interoperable. Once completed, the databases would provide a valuable resource for identifying criminals and terrorists trying to illegally obtain driver's licenses and identification cards.

---

[272] Anil K. Jain, "Mutilmodal Interfaces that Flex, Adapt and Persist," *Communications of the ACM*, 2004, Volume 47, Issue 1: 34–40, 37–38.

[273] Anil Jain, Karthik Nandakumar and Arun Ross, "Score Normalization in Multimodal Biometric Systems," *Pattern Recognition: The Journal of the Pattern Recognition Society*, 2005: 2270–2285, 2283.

[274] Damien Dessimoz, Jonas Richiardi, Christophe Champod and Andrzej Drygajlo, "Multimodal Biometrics for Identity Documents," *Forensic Science International* , 2006: 154–159, 155.

Currently, India recognizes 20 different proofs of identity, such as ration cards, passports, birth certificates, and driver's licenses, yet many poor individuals have no form of identification and are unable to open a bank account or apply for government assistance. To address the problem of large numbers of citizens who currently have no proof of identity, assist with illegal immigration policy enforcement and help guard against foreign terrorists, including the Pakistanis that launched a commando attack on Mumbai, India, has initiated a national multimodal biometric identification program.[275] Within the next five years, India will provide all 1.2 billion citizens with a national identity number, similar to a Social Security number, and a biometric identity card.[276] The biometric identity card will have finger, face and iris biometric information. The data will be stored online, creating the largest biometric database in the world.[277] India's development of a multimodal biometric identification system to support 1.2 billion people is an indication that the technology is scalable to support very large populations, as would be required to support a U.S. national identification system. Development of a multimodal biometric driver's license and identification card system within the U.S. is a viable technical option.

b. Biometric Alternatives

This section briefly analyzes whether the biometric technologies identified as being best suited for use in national security and border security purposes are viable options for incorporation into a national identification system. Fingerprinting has been used for decades and poll data indicates that public acceptance of fingerprinting is very high. The cost of the technology is low. In an effort to better control access to theme parks, and address the inherent vulnerabilities with use of photograph identification cards, Walt Disney theme parks have been using fingerprints to secure access to parks for

---

[275] Economist World Asia, *Peering into thier Murky World*, July 2, 2009. http://www.economist.com/world/asia/displayStory.cfm?story_id=13962574 (accessed August 10, 2009).

[276] Journal of Turkish Weekly, *India Begins Project to Issue Biometric Cards to All Citizens*, September 24, 2009, http://www.turkishweekly.net/news/89600/india-begins-project-to-issue-biometric-identity-cards-to-all-citizens.html (accessed September 25, 2009).

[277] Ibid.

over a decade. The FBI, DHS and DoD have demonstrated that fingerprints can be used to identify criminals and terrorists. Government databases contain fingerprints from millions of individuals, including criminals and terrorist suspects, and could be used to assist with verification checks of all driver's license and identification card applicants. Fingerprinting technology is a viable option for a multimodal biometric national identification system.

Implementation costs are low, but there are several challenges with using hand geometry systems in a national identification system. There are not any large-scale government databases of hand geometry prints, and the fact that 1 in 100 individuals have similar hand geometry does not make hand geometry a viable option for use in a system that would need to distinguish the identity of millions of people. When compared to fingerprints, implementing a hand geometry system would be more challenging and might not provide the desired result, which is to improve national security.

The only large government databases containing iris scan biometric data is DoD's ABIS. Iris recognition systems have higher implementation costs, but iris systems do have an advantage in accuracy over both fingerprint and hand geometry systems. Another advantage to iris scan technology is that no contact with the sensor equipment is required. In an era of the H1N1 flu and concerns about pandemics, Americans might support spending additional resources to implement a highly accurate system that does not require contact. Implementation of iris scan technology nation-wide for use in a national identification system is a viable technical option, but would require a larger financial investment by states and the federal government than fingerprint technology.

Facial recognition does not require physical contact with a sensor, but the accuracy is affected by changes in lighting and obstructions such as hats, glasses or changes in appearance. The Indiana Bureau of Motor Vehicles (BMV) has effectively demonstrated that facial recognition technology can play a role in resolving identity theft. In an effort to apprehend wanted criminals, the FBI has begun using facial recognition technology to scan millions of North Carolina state driver's license photos to identify

possible matches with pictures of wanted criminals.[278] State and federal laws allow driver's license agencies to release records for law enforcement purposes, but the FBI is not authorized to store the photos.[279] Therefore, facial recognition analysis must be done at state DMVs. Facial recognition is a low-cost, viable, supplemental tool that could be used by law enforcement agencies and state DMVs to help identify identity thieves and wanted criminals.

B. COMPARISON OF ALTERNATIVES

Table 3 includes a side-by-side comparison of the alternatives. The comparison of alternatives is based on an assessment of the card cost over an eight-year period, how effectively the course of action is expected to improve security including how the option would be expected to protect identity theft, implementation feasibility, whether the option would be implemented with a central database or require integration of existing databases, primary biometric indicator required, card data storage method, assessment of political viability, and how the option would increase the cost to counterfeiting. Attributes for some of the characteristics are classified as low, medium and high as an indicator of how each alternative addresses the characteristics. The national identification using biometrics incorporates key components from REAL ID and EDL programs, including: database integration, RFID tag's and source document verification checks prior to card issuance.

[278] Mike Baker, *Associated Press: FBI Delves into DMV Photos in Search for Fugitives*, October 12, 2009. http://www.google.com/hostednews/ap/article/ALeqM5iCDKSGZjGw3GMFUml4LQLlWzNOuQD9B9O5B80 (accessed October 12, 2009).

[279] Ibid.

Characteristics	**Repeal RIA**	**RIA**	**PASS ID**	**EDL**	**National Biometric Based Identification**
Additional cost per issuance, per card	None	$8.31	Less than $8.31	$15-$30	At least the cost of an EDL card
Improves Security	Low	Medium	Low – Medium	Medium	High
Implementation Feasibility	High	Medium	Medium	Medium	Medium
Central Database or Integrated Databases	No	Yes	No	Yes	Yes
Primary Biometric Identifier(s)	Face - Photograph	Face-Photograph	Face-Photograph	Face-Photograph	Face-Photograph, Fingerprint, Iris, Facial Recognition
Data Storage on Card	Barcode or as directed by state	2-D Barcode	2-D Barcode	2-D Barcode and RFID tag	RFID tag and machine readable zone
Politically Viable	Yes	Yes	TBD	Yes	TBD
Increases cost to counterfeiting	Low	Medium	Medium	Medium	High

Table 3. Comparison of Alternatives

THIS PAGE INTENTIONALLY LEFT BLANK

V. RECOMMENDATIONS

All states issue driver's licenses and identification cards, and it could be argued that because all the states honor each other's cards, there already exists a national identification standard. A problem is that the current standard has vulnerabilities that can be exploited by criminals and terrorists, just as the 9/11 terrorists did. The RIA, and the recently-introduced PASS ID Act, address aspects of securing driver's license and identification cards, but reliance on a photograph as a biometric indicator is not sufficient to assist law enforcement and homeland security professionals with identifying criminals and terrorists before they strike. The economic impacts of another terrorist attack of the magnitude of 9/11 to the U.S. over two years are estimated at $374.7 billion.[280] Preventing another 9/11-magnitude terrorist attack and making identity theft difficult for criminals is in the national interest of all Americans.

As identity theft continues to rise each year, with costs in the billions of dollars, Americans are looking for ways to protect their identity from criminals. Relying on a driver's license with a photograph or a Social Security card with a number does not provide sufficient security for Americans. With no single trusted credential for all Americans, there is a need to implement a credential that can be presented and universally accepted for identification. This thesis argues that, based on the options available, utilizing biometric technology to secure driver's licenses and identification cards would provide a solution that addresses both national security issues and the types of identity theft requiring the presentation of a driver's license.

The 9/11 terrorist attacks forced the U.S. government and citizens to examine how civil liberties should be balanced against implementing new security measures that would improve national security. With a national biometric identification system, it will be harder for anyone to use someone else's driver's license or identification card. Therefore, establishing a national biometric-based driver's license and identification card

[280] Department of Homeland Security, *REAL ID Act Regulatory Evaluation - Final Rulemaking*, Report Identification Number: 1601-AA37, Washington D.C.: DHS, January 17, 2008, 134.

can be viewed as a privacy-enhancing technology. Professor Alan Dershowitz of the Harvard Law School, described by *Newsweek* as "the nation's most peripatetic civil liberties lawyer and one of the most distinguished defenders of individual rights," stated:

> Before 11 September 2001, I had not thought much about national identity cards. I had a knee jerk opposition to any such intrusion, growing primarily out of the misuse of identification cards by the apartheid regime in South Africa and the totalitarian regimes in the Soviet Union and China. But, the ease with which the 11 September hijackers managed to hide in open view and fall between the bureaucratic cracks made it clear to me that a foolproof national identification card had some real virtues. Then I started to think about the vices. I was hard pressed to come up with any compelling civil libertarian arguments against a simple card which would contain only five elements: the bearer's name, address, Social Security number, photograph, and a finger or retinal print matching a chip in the card…We must start thinking smartly about smart technology that can increase our security without unduly diminishing our liberty. We need not fear technology, so long as we control it, rather than allowing it to control us.[281]

The U.S. government has a responsibility to protect the nation from terrorist attack. "Balancing the equities involved and depending on the case, the benefits to the individual as well as the society of establishing a person's identity generally outweigh the costs of losing anonymity."[282] Knowing if the individual standing in front of you is who they claim to be is critical in all national security settings, whether it is screening to allow someone to board an aircraft or screening for driver's license eligibility.

The bottom line is, even with REAL ID or PASS ID, it would be easier to get on an airplane than to enter a Walt Disney theme park with an expired Disney biometrics based-access pass. Biographical information such as phone number, address and age as required on REAL IDs and PASS IDs may assist businesses and government agencies at some level with identifying individuals, but a better way to match an identification card with an individual would be to include additional biometric information.

---

[281] Alan Dershowitz, *Thinking About National ID Cards*, May 2002. http://www.homelandsecurity.org/journal/Articles/dershowitz2.htm (accessed September 11, 2009).

[282] John D. Woodward, Nicholas M. Orlans, and Peter T Higgins, *Biometrics: Identity Assurance in the Information Age,* Hightstown, New Jersey: McGraw-Hill Professional, 2002, 205.

My recommendation is to implement a national biometric identification card and would require implementation of several components, all of which are currently being implemented in part by some states and federal agencies, but have yet to be implemented on a national level. First, standardize the requirements for state driver's licenses and identification cards using RIA as a baseline, but include fingerprint and iris information, and make the requirements compulsory for states. Second, implement procedures to verify citizenship status prior to driver's license issuance, using source documents such as birth certificates, a requirement which is already required for EDLs and REAL IDs. Third, continue to integrate state DMV and federal government biometric databases, and encourage the use of facial recognition systems as a tool to identify identity thieves. Fourth, increase the federal grant funding to assist states with initial implementation.

There are legislative, policy, and funding hurdles that need to be overcome before any national identification system might be successfully implemented. The easy part for government agencies is the collection of biometric data; the hard part is how to manage the information and share it across federal agencies that have different regulations and reasons for collecting it.[283] These hurdles are not insurmountable, and can be overcome with sufficient interagency cooperation, legislative and public support. Public opinion has consistently supported implementing a national identification card system. Immediately after 9/11 and through the latest public opinion poll conducted in 2006, polls showed that between fifty-six and seventy percent of the American public supported a national identification card.[284]

The way ahead will need to be decided by U.S. citizens, the legislature and the executive branch, but there are clear alternatives, some with more security vulnerabilities than others. The U.S. has the technology and capability to implement a biometric technology solution to better secure driver's licenses and identification cards, but has not

---

[283] Stew Magnuson, "Under Watch: Government Seeking Clear Path for Biometric Data Use," *National Defense*, \September 2008, Vol. 93, Iss. 658: 23–35, 23.

[284] Pew Research Center, *Evenly Divided and Increasingly Polarized*, Political Landscape Poll, Washington D.C.: People Press, 2004, 73–74. & Pew Research Center. *News Release - Latest Poll.* December 2006 Poll Data, Washington D.C. : Peoples Press, 2006, 9–10.

been successful in implementing a robust solution similar to what India is embarking on and other countries have already implemented. Let us hope that it does not take another attack of the magnitude of 9/11 for the U.S. to implement a comprehensive solution utilizing all of the technological tools at our disposal.

APPENDIX. REAL ID ACT MATERIAL COMPLIANCE CHECKLIST[285]

1. Mandatory facial image and retention
2. Declaration of true and correct information
3. Require an individual to present at least one of the source documents for identity
4. Require documentation of date of birth; Social Security Number; address of principle residence; evidence of lawful status
5. Have a documented exceptions process
6. Reasonable efforts to make sure the individual does not have more than one license
7. Verify lawful status through the Systematic Alien Verification for Entitlements (SAVE) program or another DHS approved method
8. Verify Social Security Numbers with Social Security Administration or other DHS approved method
9. Issue driver's licenses that contain Level 1, 2, and 3 integrated security features
10. Surface of cards include full legal name, date of birth, gender, unique license number, full facial digital photograph, address of principal residence, signature, date of transaction, expiration date, and state or territory of issuance
11. Commit to mark materially compliant license with DHS approved security marking
12. Issue temporary or limited-term licenses to all individuals with temporary lawful status

[285] Senate Committee on Homeland Security and Governmental Affairs, *Impact of Implementation: A Review of the REAL ID Act and the Western Hemisphere Travel Initiative, The Material Compliance Checklist*, April 29, 2008. http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Detail&HearingID=c8bd6312-5714-4a1c-8f25-eef90c611a44, p. 360-361. (accessed July 1, 2009).

13. Have a documented security plan for Department of Motor Vehicle (DMV) operations
14. Have protections in place to ensure security of personally identifiable information
15. Require all employees handling source documents or issuing licenses to attend security awareness and fraudulent document recognition program
16. Conduct name based and fingerprint based criminal history check of DMV employees
17. Commit to be in material compliance with subparts A-D of the final regulations by January 1, 2010 or within 90 days of submitting this document
18. Clearly state on the face of non-compliant licenses that the card is not acceptable for official purposes

LIST OF REFERENCES

9/11 Commission, *9/11 and Terrorist Travel: Staff Report,* Franklin: Providence Publishing Company, August 2004.

———. *The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States,* Washington D.C. http://www.9-11commission.gov/report/911Report.pdf, 2004.

Ardis, Martin W, *Real ID Act of 2005 and its Interpretation,* Hauppauge, NY: Nova Publishers, 2005.

Aitoro, Jill, *DHS Launches Second Test of Biometric Exit Processes,* June 10, 2009. http://www.nextgov.com/nextgov/ng_20090610_9479.php (accessed June 11, 2009).

Baker, Mike, *Associated Press: FBI Delves into DMV Photos in Search for Fugitives ,* October 12, 2009. http://www.google.com/hostednews/ap/article/ALeqM5iCDKSGZjGw3GMFUml4LQLlWzNOuQD9B9O5B80 (accessed October 12, 2009).

Benson, Matthew, "Napolitano: Real ID a no-go in Arizona," *Arizona Central News,* June 18, 2008, http://www.azcentral.com/news/articles/2008/06/18/20080618real-id0618.html (accessed February 23, 2009).

Bruno, Andorra, "Immigration Legislation and Issues in the 109th Congress," CRS Report to Congress, Updated December 7, 2006.

Bush, George W, *Biometrics for Identification and Screening to Enhance National Security/NSPD-59/HSPD-24,* Washington D.C., June 5, 2008.

Campos, Elroy, *Consolidating Our Country's Biometric Resources and the Possible Implications,* Carlise Barracks: U.S. Army War College, 2008.

CNN Technology, *Scientists: RFID Chips Can Carry Viruses,* March 15, 2006. http://www.rfidvirus.org/media/cnn.com.pdf (accessed August 20, 2009).

CNN Washington D.C. Office, *Homeland Security Chief seeks to repeal REAL ID Act,* April 22, 2009, http://www.cnn.com/2009/POLITICS/04/22/real.ID.debate/ (accessed April 23, 2009).

CR80News, *Hand Geometry Verifying Sand Diego State Students Since 1998,* May 28, 2009, http://www.cr80news.com/2009/05/28/hand-readers-verifying-san-diego-state-students-since-1998 (accessed September 4, 2009).

Curtius, Mary, *GOP Push for Immigration Curbs*, January 27, 2005, http://articles.latimes.com/2005/jan/27/nation/na-immig27 (accessed August 4, 2009).

Data Privacy & Integrity Advisory Committee, "The Use of RFID for Human Identity Verification," *DHS.gov*. December 6, 2006, http://www.dhs.gov/xlibrary/assets/privacy/privacy_adcom_12-2006_rpt_RFID.pdf (accessed August 17, 2009).

Defense Threat Reduction Agency, *Military Critical Technologies List: Information-Security Technology*, Ft. Belvoir, VA: Department of Defense, October 2003.

Department of Homeland Security (DHS), *Privacy Impact Assessment for the Use of Radio Frequency Identification Technology for Border Crossings*, Washington D.C.: DHS, January 22, 2008.

Department of Homeland Security, *DHS Issues Proposal for States to Enhance Driver's Licenses*, March 1, 2007, http://www.dhs.gov/xnews/releases/pr_1172765989904.shtm (accessed April 15, 2009).

———. *Enhanced Driver License: What are they? ,* June 2009. http://www.dhs.gov/xtrvlsec/crossingborders/gc_1197575704846.shtm (accessed June 4, 2009).

———. "Fact Sheet on Enhanced Driver's Licenses," *U.S. Customs and Border Protection*, May 29, 2009, http://www.cbp.gov/linkhandler/cgov/travel/vacation/enhanced_dl_fs.ctt/enhanced_dl_fs.doc (accessed August 19, 2009).

———. "Final Rule: Minimum Standards for Driver's Licenses and Identifcation Cards Acceptable by Federal Agencies for Official Purposes," *Federal Register, Volume 73, Number 19*, January 28, 2008, http://edocket.access.gpo.gov/2008/08-140.htm (accessed July 1, 2009).

———. Notice of Proposed Rulemaking, "Minimum Standards for Driver's Licenses and Identification Cards Acceptable to Federal Agencies for Official Purposes," *DHS. REAL ID Act of 2005*, March 2007. http://www.dhs.gov/xlibrary/assets/nprm_realid.pdf (accessed July 26, 2009).

———. *Publication of Western Hemisphere Travel Initiative*, March 27, 2008. http://www.dhs.gov/xnews/releases/pr_1206635771151.shtm (accessed April 10, 2009).

———. *Public Law 109-13 109th Congress,* April 10, 2009. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_public_laws&docid=f:publ013.109 (accessed April 10, 2009).

———. *REAL ID Act Regulatory Evaluation - Final Rulemaking,* Report Identification Number: 1601-AA37, Washington D.C.: DHS, January 17, 2008.

———. *REAL ID: States Granted Extensions,* November 10, 2008. http://www.dhs.gov/files/programs/gc_1204567770971.shtm#3 (accessed June 21, 2009).

———. *US-VISIT Travelor Information ,* May 29, 2009, http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0006.shtm (accessed June 16, 2009).

Department of Homeland Security Office of the Inspector General, "Potentially High Costs and Insufficient Grant Funds Pose a Challenge to REAL ID Implementation," OIG-09-36, Washington D.C., March 2009.

Department of the Army, *DoD Biometrics Task Force Homepage,* 21 2009, May, http://www.biometrics.DoD.mil/ (accessed May 21, 2009).

Dershowitz, Alan, *Thinking About National ID Cards,* May 2002, http://www.homelandsecurity.org/journal/Articles/dershowitz2.htm (accessed September 11, 2009).

Dessimoz, Damien, Richiardi, Jonas, Champod, Christophe and Drygajlo, Andrzej, "Multimodal Biometrics for Identity Documents," *Forensic Science International*, 2006: 154–159.

Division B—REAL ID Act of 2005, the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, Pub. L. 109-13, 119 Stat. 231, 302 (2005) (codified at 49 U.S.C. 30301).

Economist World Asia, *Peering into their Murky World,* July 2, 2009, http://www.economist.com/world/asia/displayStory.cfm?story_id=13962574 (accessed August 10, 2009).

Electronic Frontier Foundation, *Biometrics: Who is Watching You?,* September 2003. http://www.eff.org/wp/biometrics-whos-watching-you (accessed May 21, 2009).

Electronic Privacy Information Center, "REAL ID Implementation Review Few Benefits, Staggering Costs," *epic.org.* May 2008, http://epic.org/privacy/id-cards/ (accessed April 19, 2009).

Federal Trade Commission, "Consumer Sentinel Data Book January - December 2008," *www.ftc.gov.* February 26, 2009, http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf (accessed July 14, 2009).

Fuller, Andrea, *Effort to Replace Federal Driver's License Mandate Gains,* July 16, 2009, http://www.nytimes.com/2009/07/16/us/16identify.html (accessed July 16, 2009).

GlobalSecurity.org., *Homeland Security: Biometrics,* June 2009, http://www.globalsecurity.org/security/systems/biometrics.htm (accessed June 1, 2009).

Gugliotta, Guy, *The Eyes Have It: Body Scans at the ATM,* June 21, 1999, http://www.washingtonpost.com/wp-srv/national/daily/june99/scans21.htm (accessed May 21, 2009).

Harmel, Karen, *Walt Disney World: The Government's Tomorrowland?,* September 1, 2006, http://newsinitiative.org/story/2006/09/01/walt_disney_world_the_governments (accessed September 4, 2009).

Harper, Jim, "Understanding the Realities of REAL ID," *Vital Speeches of the Day*, May 2007: 208–212.

Harris, Shon, *CISSP All-in-One Exam Guide,* New York : McGraw-Hill Publishing, 2007.

Hedgepeth, William Oliver, *RFID Metrics: Decision Making Tools for Today's Supply Chains,* Boca Raton: CRC Press, 2007.

Howe, James, "Defeating the Unknown Terrorist," *Proceedings*, October 2008, Vol. 134, Iss. 10: 38–42.

Hsu, Spencer, *Administration Plans to Scale Back REAL ID Law,* June 14, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/06/13/AR2009061302036.html (accessed September 21, 2009).

Hudson, Audrey, "Napolitano Debates Real ID," *The Washington Times*, February 20, 2009, http://www.washingtontimes.com/news/2009/feb/20/napolitano-debates-real-id/ (accessed February 23, 2009).

Identity Theft 911 Knowledge Center, *Expanding RFID Use Raises Privacy Concerns,* July 22, 2009, http://identitytheft911.org/alerts/alert.ext?sp=10911 (accessed August 17, 2009).

Imperial Valley News - Yuma, AZ, *Program Broadened to Enhance Identification and Removal of Criminal Aliens,* June 16, 2009, http://www.imperialvalleynews.com/index.php?option=com_content&task=view&id=5910&Itemid=1 (accessed June 16, 2009).

Indiana Bureau of Motor Vehicles, *Identity Thieves Caught By DMV,* August 9, 2009, http://www.in.gov/bmv/5168.htm (accessed August 9, 2009).

———. *Why is Secure ID Necessary?,* August 9, 2009, http://www.in.gov/bmv/5141.htm (accessed August 9, 2009).

International Biometric Group, *Biometrics in Driver's License Operations,* Analysis of Driver Licenses and Biometrics, Washington D.C.: IBG Research Consulting Integration, 2002.

Jain, A.K., R. Bolle, and S. Pankanti, *Biometrics: Personal Identification in Networked Society,* London: Kluwer Academic Publishers, 1999.

Jain, Anil K, "Mutilmodal Interfaces that Flex, Adapt and Persist," *Communications of the ACM*, 2004, Volume 47, Issue 1: 34–40.

Jain, Anil K., Flynn, Patrick, and Abraham, Arun Ross, *Handbook of Biometrics*, New York: Springer, 2007.

Jain, Anil, Nandakumar, Karthik, and Ross, Arun, "Score Normalization in Multimodal Biometric Systems," *Pattern Recognition: The Journal of the Pattern Recognition Society*, 2005: 2270–2285.

Johnson, Carolyn, *Spotting a Terrorist: Next-Generation System for Detecting Suspects in Public Settings Holds Promise, Sparks Privacy Concerns,* September 18, 2009, http://www.boston.com/news/local/massachusetts/articles/2009/09/18/spotting_a_terrorist/ (accessed September 22, 2009).

Journal of Turkish Weekly, *India Begins Project to Issue Biometric Cards to All Citizens,* September 24, 2009, http://www.turkishweekly.net/news/89600/-india-begins-project-to-issue-biometric-identity-cards-to-all-citizens.html (accessed September 25, 2009).

Keeton, Ann, "Fingerprints Give a Hand to Security: Verifying Identities Through Biometrics is Poised to Expand," *Wall Street Journal*, Apr 12, 2007: B.4.

Kephart, Janice, *Secretary Chertoff's Stocking Stuffer: States Get Infusion of Secure ID Monies,* December 19, 2008, http://cis.org/kephart/chertoffsstockingstuffer (accessed September 21, 2009).

Kephert, Janice L. and Jena Baker McNeil, *The PASS ID Act: Rolling Back Security Standards for Driver's License*, Background Report on REAL ID Act and PASS ID Act, Washington D.C.: The Heritage Foundation, 2009.

Kremen, Rachel, *Touchless 3-D Fingerprinting: A New System Offers Better Speed and Accuracy*, September 30, 2009, http://www.technologyreview.com/computing/23549/page1/ (accessed October 1, 2009).

Lawlor, MaryAnn, "Bureau Beefs Up Biometrics Capabilities," *Signal*, September 2008, Vol. 63, Iss. 1: 67–70.

Lewan, Todd, *Special Alloy Sleeves Urged to Block Hackers? ,* July 11, 2009, http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2009/07/11/financial/f113716D08.DTL (accessed August 19, 2009).

Lewen, Todd, "ID Chips Raise Privacy Issues," *The Herald*, July 12, 2009: A1 and A9.

Lipowicx, Alice, *DHS Expands RFID use at Borders Today*, June 1, 2009, http://www.fcw.com/Articles/2009/06/01/DHS-expands-RFID-use-at-borders-today.aspx (accessed August 15, 2009).

Lowe, Christian, *Biometrics Track Bad Guys*, February 23, 2007, http://www.defensetech.org/archives/003306.html (accessed May 22, 2009).

Magnuson, Stew, "Under Watch: Government Seeking Clear Path for Biometric Data Use," *National Defense*, September 2008, Vol. 93, Iss. 658: 23–35.

Martin, Zack, *Biometrics and the Department of Defense*, September 16, 2009. http://www.secureidnews.com/2009/09/16/biometrics-and-the-department-of-defense (accessed September 18, 2009).

———. *New Driver License Legislation Proposed*, September 19, 2009, http://www.secureidnews.com/2009/09/19/new-driver-license-legislation-proposed (accessed September 24, 2009).

———. *Smart Card, Biometrics on the way for Social Security card?*, July 22, 2009. http://www.digitalidnews.com/2009/07/22/smart-card-biometrics-on-the-way-for-social-security-card (accessed July 24, 2009).

Matkin, Michael, *Biometric Database Offers Security Stamp of Approval*, August 10, 2009, http://www.af.mil/news/story.asp?id=123162638 (accessed September 10, 2009).

Merserve, Jeanne and Mike Ahlers, *9/11 Commission Members Act to Finally Wrap it up,* July 25, 2009, http://www.cnn.com/2009/US/07/25/new.antiterror.group/index.html (accessed July 25, 2009).

Morgan, Daniel and William Krouse, *Biometric Identifiers and Border Security: 9/11 Commission Recommendations and Related Issues,* Report Number: RS21916, Washington D.C.: Congressional Research Service (CRS) Report for Congress, 2005.

Nakishima, Ellen, *Post 9/11 Dragnet Turns Up Surprises: Biometrics Links Foreign Detainees to Arrests in the U.S,* July 6, 2008, http://www.biometrics.dod.mil/Newsletter/issues/2008/July/v4issue3/v4issue3_add3.html (accessed May 15, 2009).

National Archives and Records Administration, "Department of Homeland Security: 6 CFR Part 37, Docket No. DHS-2006-0030, Minimum Standards for Driver's Licenses and Identification Cards," *Federal Register*, March 2007, 2007, http://edocket.access.gpo.gov/2007/pdf/07-1009.pdf (accessed July 21, 2009).

National Governors Association, National Conference of State Legislatures, American Association of Motor Vehicle Administrators, *The REAL ID Act: Nationl Impact Analysis,* Washington D.C.: AAMVA, September 2006.

National Institute of Standards and Technology (NIST), *National and International Biometric Standards - Development Bodies and Published Standards,* February 2009, http://www.itl.nist.gov/div893/biometrics/standards.html (accessed April 21, 2009).

National Science and Technology Council, "Biometrics Foundation Documents," *Committee on Homeland and National Security,* August 2006, http://www.biometrics.gov/Documents/biofoundationdocs.pdf (accessed September 2, 2009).

———. "Facial Recognition," *Committee on Homeland and National Security,* August 7, 2006, http://www.biometrics.gov/Documents/FaceRec.pdf (accessed September 11, 2009).

———. "Iris Recognition," *Committe on Homeland and National Security,* August 7, 2006, http://www.biometrics.gov/Documents/IrisRec.pdf (accessed September 12, 2009).

———. "Hand Geometry," *Committee on Homeland and National Security, Subcommittee on Biometrics ,* August 6, 2006, http://www.biometrics.gov/Documents/HandGeometry.pdf (accessed September 2, 2009).

Osborne, James, *10th Amendment Movement Aims to Give Power Back to States,* May 26, 2009, http://www.foxnews.com/politics/2009/05/26/tenth-amendment-movement-aims-power-states/ (accessed July 10, 2009).

Pew Research Center, *Evenly Divided and Increasingly Polarized,* Political Landscape Poll, Washington D.C.: People Press, 2004.

———. *News Release - Latest Poll,* December 2006 Poll Data, Washington D.C.: Peoples Press, 2006.

———. *No Change in Views of Torture, Warrantless Wiretaps,* February 2009 News Release - Poll, Washingt D.C.: Peoples Press, 2009.

Radia, Kirit. *Passports Go High-Tech,* August 14, 2006, http://i.abcnews.com/Politics/Story?id=2313170&page=1 (accessed September 28, 2009).

Reid, Paul. *Biomtrics for Network Security* , Upper Saddle River, New Jersey: Prentice Hall, 2004.

Reuters - Latest News. *Unisys Announces Successful Multi-Vendor Interoperability of Iris Recognition Technology for Homeland Security,* September 21, 2009, http://www.reuters.com/article/pressRelease/idUS73560+21-Sep-2009+BW20090921 (accessed September 24, 2009).

RFID Journal, *What is RFID?,* August 14, 2009, http://www.rfidjournal.com/article/articleview/1339/1/129/ (accessed August 15, 2009).

———. *The Basics of RFID Technology,* August 5, 2009, http://www.rfidjournal.com/article/print/1337 (accessed August 14, 2009).

Rubin, Joel, *Counter-terrorism Investigators Find Alleged Identity Theft Ring,* July 26 , 2009, http://www.latimes.com/entertainment/news/music/la-me-fraud26-2009jul26,0,7924251.story?track=rss (accessed July 27, 2009).

Schneier, Bruce, *Does Big Brother Want to Watch?,* October 4, 2004, http://www.schneier.com/essay-060.html (accessed August 18, 2009).

———. *The ID Chip You Don't Want in Your Passport,* September 16, 1006, http://www.washingtonpost.com/wp-dyn/content/article/2006/09/15/AR2006091500923.html (accessed September 7, 2009).

———. *Will REAL ID Actually Make Use Safer? An Examination of Privacy and Civil Liberty Concerns,* May 8, 2007, http://www.schneier.com/testimony-realid.html (accessed May 21, 2009).

Science Daily News, *New Biometric ID: A Quick X-Ray Snapshot of a Person's Knee,* March 28, 2009, http://www.sciencedaily.com/releases/2009/03/090325150611.htm (accessed May 1, 2009).

Senate Committe on Homeland Security and Governmental Affairs, "DHS Secretary Janet Napolitano," *Hearings: Identification Security, Reevaluating REAL ID,* July 15, 2009, http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=3d9a52cd-c442-4dee-9a1f-b02ed3b38000 (accessed July 17, 2009).

———. *Impact of Implementation: A Review of the REAL ID Act and the Western Hemisphere Travel Initiative: Costs and Privacy Concerns,* April 29, 2008, p. 360, http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Detail&HearingID=c8bd6312-5714-4a1c-8f25-eef90c611a44 (accessed July 10, 2009).

———. *Secure Identification Fix Clears Committee,* July 29, 2009, http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord_id=c7f85c1e-5056-8059-76ef-4b4cb7649086&Region_id=&Issue_id=716b4c83-7747-4193-897b-632e5c281a91 (accessed July 30, 2009).

———. *Web Cast of July 15, 2009 Identification Security: Reevaluating the REAL ID Act: (25 Minute Mark),* July 15, 2009, http://www.senate.gov/fplayers/I2009/urlPlayer.cfm?fn=govtaff071509&st=1405&dur=10560 (accessed July 17, 2009).

———. "David Quam, Director of Federal Relations, National Governors Association," *Hearings: Identification Security, Reevaluating REAL ID,* July 15, 2009, http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=3d9a52cd-c442-4dee-9a1f-b02ed3b38000 (accessed July 17, 2009).

Service Representative, Michigan Department of State, data provide to author, *Questions on Enhanced Driver's License,* (September 28, 2009).

Severens, John, *AETC Officials to Automate Entry Control,* May 7, 2009, http://www.af.mil/news/story.asp?id=123148134 (accessed May 20, 2009).

Smartrac Group, *e-Passport RFID's,* July 14, 2009, http://www.smartrac-group.com/en/personalausweise.php (accessed August 15, 2009).

Souder, Mark, *Why we need ID's with Biometric Indicators* , January 10, 2008, http://souder.house.gov/index.cfm?FuseAction=NewsCenter.Articles&ContentRecord_id=69f68198-19b9-b4b1-1237-e37db00e6ddd&Region_id=&Issue_id=67cc589f-7e9c-9af9-7359-9a4ae482194b (accessed July 3, 2009).

Sperling, Ed, *Forbes: Future of Digital ID's*, May 11, 2009, http://www.forbes.com/2009/05/11/biometrics-security-enterprise-technology-cio-network-biometrics.html (accessed May 13, 2009).

St. John, Warren, *In the ID Wars, the Fakes Gain*, March 6, 2005, http://www.nytimes.com/2005/03/06/fashion/06fake.html?_r=1&pagewanted=print&position= (accessed July 14, 2009).

Staff Report of the National Commission on Terrorist Attacks Upon the United States, *9/11 and Terrorist Trave* , Franklin, TN: Providence Publishing Corporation, 2004.

State of Michigan Department of State, *Enhanced Driver's Licenses Arrive*, April 21, 2009, http://www.michigan.gov/sos/0,1607,7-127--213322--,00.html (accessed August 15, 2009).

Stelter, Leischen, *Biometrics to Ensure Parents Leave with the Right KID's*, August 11, 2009, http://www.securitydirectornews.com/?p=article&id=sd20090896kXm7 (accessed September 12, 2009).

Sundeen, Matt, "The REAL ID Rebellion," *State Legislatures*, Mar 2008; 34, 3: 26–28.

Swartz, Nikki, "REAL ID to Cost $11 Billion Plus," *Information Management Journal*, Jan/Feb 2007; 41, 1.

Sykes, Charlie, *Senenbrenner Smacks A Clueless Napalitano*, April 22, 2009, http://www.620wtmj.com/shows/charliesykes/43478517.html (accessed May 10, 2009).

Tenth Amendment, *The Charters of Freedom: Bill of Rights*, August 11, 2009, http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html (accessed August 11, 2009).

Thompson, Jenna, *Hand Scanners Bring Convenience to SLC*, September 9, 2009, http://www.baylor.edu/lariat/news.php?action=story&story=60983 (accessed September 10, 2009).

Tipton, Harold F., and Krause, Micki, *Information Security Management Handbook, Sixth Edition*, Boca Raton: CRC Press, 2007.

U.S. Department of the Army, "Biometrics Task Force: DoD ABIS," *BTF Trifold.*

United States Census Bureau, *Vermont 2008 Population Estimate,* September 4, 2009, http://quickfacts.census.gov/qfd/states/50000.html (accessed September 14, 2009).

United States Customs and Border Patrol, *Learn to Use Your RFID Enabled Documents,* May 11, 2009, http://www.cbp.gov/xp/cgov/newsroom/multimedia/video/travel_videos/rfid_enabled/ (accessed September 11, 2009).

United States Department of State, *Passports,* August 17, 2009, http://travel.state.gov/passport/passport_1738.html (accessed August 17, 2009).

———. *U.S. Passport Card,* August 17, 2009, http://travel.state.gov/passport/ppt_card/ppt_card_3926.html (accessed August 18, 2009).

———. *U.S. Passport Card Frequently Asked Questions,* May 2009, http://travel.state.gov/passport/ppt_card/ppt_card_3921.html (accessed August 15, 2009).

United States General Accounting Office, *Technology Assessment: Using Biometrics for Border Security,* Washington D.C.: GAO, November 2002.

United States Government Accountability Office, *Homeland Security: US-VISIT Program Planning and Execution Improvements Needed*, Report to Congressional Commities, Washington D.C. : U.S. GAO, December 2008.

———. *Information Security: Radio Frequency Identification Technology in the Federal Government,* Washington D.C.: U.S. GAO, May 2005.

United States Immigration and Customs Enforcement . *ICE: Secure Communities Program* , May 14, 2009, http://www.ice.gov/pi/news/factsheets/secure_communities.htm (accessed May 21, 2009).

Watanabe, Teresa, *Worker ID Cards Expected to Get a New Look*, June 19, 2009, http://articles.latimes.com/2009/jun/16/nation/na-worker-id16 (accessed July 15, 2009).

Wayman, James, *National Biometrics Test Center: Biometrics Publications*, 2000, http://www.engr.sjsu.edu/biometrics/publications_tech.html (accessed May 20, 2009).

Woodward, John D., Nicholas M. Orlans, and Peter T. Higgins, *Biometrics: Identity Assurance in the Information Age.* Hightstown, New Jersey: McGraw-Hill Professional, 2002.

Ya Ni, Anna and Tat-Kei Ho, Alfred. "A Quiet Revolution or a Flashy Blip? The REAL ID Act and U.S. National Identification System Reform." *Public Administration Review*, Nov/Dec 2008; 68, 6.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California